McAfee® Network Security Platform (NSP) Security Target

Release Date:	January 10, 2012
Document ID:	10-2280-R-0044
Version:	1.1

Prepared By:	InfoGard Laboratories, Inc.
Prepared For:	McAfee, Incorporated 2821 Mission College Blvd Santa Clara, California 95054

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), conformance claims, ST organization and terminology. It also includes an overview of the evaluated product.

1.1 Security Target Reference

The Security Target reference shall uniquely identify the Security Target.

ST Title:	McAfee Network Security Platform Security Target
ST Version Number:	Version 1.1
ST Author(s):	Ryan Day
ST Publication Date:	January 10, 2012

1.2 Target of Evaluation Reference

The Target of Evaluation reference shall identify the Target of Evaluation.

TOE Developer	McAfee, Incorporated 2821 Mission College Blvd Santa Clara, California 95054
TOE Identification:	McAfee Network Security Platform
TOE Version	6.1

The TOE is comprised of one or more of the sensors listed below and the Network Security Manager (NSM) Version 6.1

Model Number	Part Number	Revision
Sensor M-1450	600-1230-03-G	C
Sensor M-1250	600-1231-03-G	D
Sensor M-2750	600-1209-02-G	D
Sensor M-2850	600-1470-01-G	C
Sensor M-2950	600-1429-01-G	D
Sensor M-6050	600-1220-06-G	C
Sensor M-4050	600-1245-05-G	C
Sensor M-3050	600-1246-05-G	C
Sensor M-8000	600-1221-06-G (Primary) 600-1222-06-G (Secondary)	C C
Sensor I-4010	600-0022-05-G5	E

Sensor I-4000	600-0001-10-G5	D
Sensor I-3000	600-0023-05-G5	E
Sensor I-2700	600-1000-04-G5	D
Sensor I-1400	600-0019-03-G5	D
Sensor I-1200	600-0006-02-G5	E

Note: M-Series sensors must be ordered with the FIPS option to meet the Common Criteria claims.

1.3 Organization

- **Security Target Introduction (Section 1) –** Provides identification of the TOE and ST, an overview of the TOE, an overview of the content of the ST and relevant terminology. The introduction also provides a description of the TOE security functions as well as the physical and logical boundaries for the TOE, the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.
- **Conformance Claims (Section 2) –** Provides applicable Common Criteria (CC) conformance claims, Protection Profile (PP) conformance claims and Assurance Package conformance claims.
- **Security Problem Definition (Section 3) –** Describes the threats, organizational security policies, and assumptions pertaining to the TOE and the TOE environment.
- **Security Objectives (Section 4) –** Identifies the security objectives for the TOE and its supporting environment as well as a rationale that objectives are sufficient to counter the threats identified for the TOE.
- **Extended Components Definition (Section 5) –** Presents components needed for the ST but not present in Part II or Part III of the Common Criteria Standard.
- **Security Requirements (Section 6) –** Presents the Security Functional Requirements (SFRs) met by the TOE and the security functional requirements rationale. In addition this section presents Security Assurance Requirements (SARs) met by the TOE as well as the assurance requirements rationale. Provides pointers to all other rationale sections, to include the rationale for the selection of IT security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- **Summary Specification (Section 7) –** Describes the security functions provided by the TOE that satisfy the security functional requirements, provides the rationale for the security functions. It also describes the security assurance measures for the TOE as well as the rationales for the assurance measures.

1.4 Document Terminology

Please refer to CC v3.1 Part 1 Section 4 for definitions of commonly used CC terms.

1.4.1 ST Specific Terminology

Alert

An alert is a notification of a system event, attack or other incident that triggers the intrusion Detection System.

Authorized Administrator(s)

A general term used in this ST to refer to administrative users holding the Security Administrator, Audit Administrator, or Crypto Administrator roles.

Attack

A set of actions performed by an attacker that poses a threat to the security state of a protected entity in terms of confidentiality, integrity, authenticity, availability, authorization and access policies.

CIDR

(Classless Inter-Domain Routing) is a scheme which allocates blocks of Internet addresses in a way that allows summarization into a smaller number of routing table entries. A CIDR address contains the standard 32-bit IP address but includes information on how many bits are used for the network prefix.

Denial of Service

In a Denial of Service (DoS) attack, the attacker attempts to crash a service (or the machine), overload network links, overload the CPU, or fill up the disk. The attacker does not always try to gain information, but to simply act as a vandal to prevent the user from making use of the machine.

Distributed DoS (DDoS)

These attacks usually consist of standard DoS attacks orchestrated by attackers covertly controlling many, sometimes hundreds of different machines.

HTTPS

The secure hypertext transfer protocol (HTTPS) is a communications protocol designed to transfer encrypted information between computers over the World Wide Web. HTTPS is http using Secure Socket layer (SSL) or Transport Layer Security (TLS) encryption.

Intrusion

Unauthorized access to, and/or activity in, an information system, usually for the purpose of tampering with or disrupting normal services. See also Attack.

Intrusion Detection

The process of identifying that an intrusion was attempted is in process or has occurred.

NTP

Network Time Protocol provides a mechanism to synchronize time on computers across the internet. The specification for NTP version 3 is defined in RFC 1305. Such synchronization can be very useful for multi-machine activities that depend upon accurate time stamps.

Policy

A user-configured security rule that determines the permission of traffic across a network. Policies can set rules for protocols (HTTP, UDP), machines (NT, Solaris), operating systems (UNIX), and other types of network information. A policy also defines what actions should be taken in the event of non-permissible activity.

Policy Violations

All activities for which the underlying traffic content may not be malicious by itself, but are explicitly forbidden by the usage policies of the network as defined by a security policy. These can include “protocol violations” wherein packets do not conform to network protocol standards.

Port Cluster

Port Cluster is a more intuitive term for an Interface Group. An interface group enables multiple sensor ports to be grouped together for the effective monitoring of asymmetric environments. Interface groups normalize the impact of traffic flows split across multiple interfaces, thus maintaining state to avoid information loss. Once configured, an interface group appears in the Resource Tree as a single interface node (icon) under the sensor where it is located. All of the ports that make up the interface are configured as one logical entity, keeping the configuration consistent.

MySQL Database

A Relational database that allows for the definition of data structures, storage/retrieval operations and integrity constraints. The data and relations between them are kept in organized tables, which are collections of records and each record in a table contains the same fields.

Roles

A class of user privileges that determines the authorized activities of the various users in the system.

Sensor

The sensor is a network device containing the intrusion detection engine. It analyzes network traffic and searches for signs of unauthorized activity.

Signature

Activities or alterations to an information system indicating an attack or attempted attack, detectable by examination of audit trail logs.

Span Mode

One of the monitoring modes available for an NSP sensor. In the SPAN mode, the sensor functions by mirroring the packet information on a switch or hub and sending the information to a sensor for inspection, while continuing the transmission of traffic with negligible latency. SPAN mode is typically half-duplex, and works through a connection of a sensor to a port on a hub or the SPAN port of a switch.

SPAN Port

On a switch, SPAN mirrors the traffic at one switched segment onto a predefined port, known as a SPAN port.

Threat Analyzer

A graphical user interface (GUI) for viewing specific attack information in the NSM System. The Threat Analyzer interface is part of the NSM component, and focuses on alert forensic analysis.

TLS

Transport Layer Security (TLS) is a cryptographic protocol used for communications over networks. TLS is used to encrypt segments of a network.

Tap

A tap is hardware device that passes traffic unidirectionally from a network segment to the IDS. Traffic is mirrored as it passes through the tap. This mirror image is sent to the IDS for inspection. This prevents traffic passing from being directed at the IDS.

Tap Mode

One of the monitoring modes available for an NSP sensor. In this mode, the NSP functions by mirroring the packet information and sending the information to a sensor for inspection, while continuing the transmission of traffic with negligible latency. Tap mode works through installation of an external wire tap, a port on a hub, or the SPAN port of a switch. This is also known as passive monitoring mode.

Trojan Horse

A malware computer program that appears to perform a useful function, but instead facilitates unauthorized access of the user's computer system.

Virtual IDS

Virtual IDS (VIDS) is an NSM feature that enables you to logically segment a sensor into a large number of virtual sensors, each of which can be customized with its own security policy. VIDS are represented in the NSM as *interfaces* and *sub-interfaces*.

VLAN

Virtual Local Area Network. A logical grouping of two or more nodes which are not necessarily on the same physical network segment, but which share the same network number. This is often associated with switched Ethernet networks.

Vulnerability

Vulnerability is a weakness which allows an attacker to reduce a system's Information Assurance by exploiting a system susceptibility or flaw.

Exclusive OR

XOR is a logical operator that results in true if one of the operands (not both) is true.

SNORT

Snort® is an open source network intrusion prevention and detection language (IDS/IPS) developed by Sourcefire.

1.4.2 Acronyms

CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System

I/O	Input/Output
MIB	Management Information Base
NIST	National Institute of Standards and Technology
NSM	Network Security Manager
NSP	Network Security Platform (TOE system)
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

1.5 Common Criteria Product type

The TOE is classified as an **Intrusion Detection System (IDS).**

1.6 TOE Overview

The intended usage of the TOE is to perform stateful inspection on a packet basis to discover and prevent intrusions, misuse, denial of service (DoS) attacks, and distributed denial of service (DDoS) attacks. McAfee Incorporated offers various types of sensor appliances providing different bandwidth and deployment strategies. These are the models listed in section 1.2.

The Network Security Manager (NSM) software is used to configure and manage an NSP deployment. The NSM is a set of applications coupled with an embedded MySQL Database. The MySQL Database is installed on the same platform as the NSM installation.

The McAfee Incorporated Update Server is a McAfee-owned and operated file server that provides updates to the signature files and software of NSP sensors in customer installations. The Update Server resides at McAfee Incorporated facilities. Note: Software updates beyond signature updates, such as those to update the core NSP software suite, are excluded for the CC Evaluated Configuration.

1.7 Target of Evaluation Description

The NSP IDS product is a combination of network appliances and software built for the detection of intrusions, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks and network misuse.

The NSP IDS system is composed of a family of sensor appliances and an NSP management platform referred to as an NSM. The sensor appliances are stand-alone appliances from McAfee

Incorporated. All other components of the product are software only components that run on Windows.

The NSM management platform is an IDS management solution for managing NSP sensor appliance deployments for large and distributed enterprise networks. Access to the NSM is limited to a Console Machine. Access to the NSM requires authentication using certificate credentials obtained from a Common Access Card (CAC) in the Operational Environment. Certificates presented via the CAC are checked for revocation status using an OCSP server in the Operational Environment. The NSM operates with a MySQL Database to persist configuration information and alert data. NSM for Windows Server 2008 includes the MySQL database.

1.8 Product Features

The Sensor Subsystem performs:

- *Traffic Capture* captures packets into a data store for review.
- *Load balancing and protocol verification* makes security decisions such that it can filter packets of no interest.
- *Denial of Service detection and response* detects DoS attacks and provides an alert capability and the capability to drop packets identified that are part of the DoS attack.
- *Signature detection and anomaly detection* performs anomaly detection, logs attack information and performs response functions. The response functions include the following: alert generation, packet logging, TCP reset, ICMP host unreachable, forward blocking (Quarantine), alert filtering and dropping of packets. Smart Blocking technology reduces the likelihood of false-positives by identifying attacks and associating a confidence level for each identified attack.
- *Sensor management* is the interface between the sensor and the NSM. It has the responsibility to push policies that have been defined in the Management Subsystem to the appropriate sensor module.

The NSM provides management functions to manage NSP sensor appliance deployments. The NSM is a web-based security management system.

The NSM provides an interface to the sensor referred to as the NSM console. The NSM console is a web-enabled application that runs on a client platform.

The TOE offers file-based analysis and blocking of known malicious payloads. The sensor creates hashes of suspect files being transmitted through the sensor and compares the hash against a database of known malicious files (payloads containing viruses, malware, etc.). This database is updated by the McAfee update server. [1]

The Threat Analyzer performs real-time alert analysis. This analysis provides intelligent management and analysis of alerts in real time with granular drill-down capabilities and color-

[1] Artemis functionality is only available using M-Series sensors.

coding that enable the administrators to quickly pinpoint the target, source, and severity of network attacks.

The management features provided by the NSM include the following:

- Threat Updates: An Update Server controlled by McAfee Incorporated delivers signature updates without requiring sensor reboots, providing protection against newly-discovered attacks.
- Granular Security Policy Management: Flexible and custom policy management per sensor — from multiple network segments to individual hosts — delivers improved attack detection and prevention.
- Administrative Domains: Scalable security policy administration with role-based access control allows delegation of administrative responsibilities.
- Forensic Analysis: Analysis tools, including enable detailed historical and real-time forensic analysis to determine network attack patterns.
- Response management: A set of response actions — including user-defined responses and notification capabilities — provide proactive attack notification and prevention.

The McAfee Incorporated Update Server is a McAfee Incorporated owned and operated file server that makes available updates of the signature files of NSP sensors in customer installations. These new signature files are available through the internet.

The TOE supports SSL encrypted traffic and enforces all functionality of this traffic on selected sensor models. Through the management interface, the Administrator can import up to 64 certificates to allow the TOE to decrypt and analyze traffic passing through the sensor.

The TOE can be configured to perform file-based analysis of traffic in search of malicious payloads. The TOE communicates (through the DNS server) with the Artemis database to identify malicious files. Additionally, an Administrator can import customized hashes of files to store locally for malicious payload analysis. This functionality (collectively known as Artemis analysis) is managed and deployed through the manager.[2]

The TOE includes a User Defined Signature (UDS) feature in the form of an editor utility that allows Administrative users to create attack instances with signatures for implementation in the Network Security Platform (NSP) policy enforcement process. This allows for the development of custom signatures based on deployment particular threats and circumstances. The TOE also allows for open-source or third-party SNORT signatures to be imported and converted into UDS signatures.

1.9 Physical Boundaries

The components of the Network Security Platform are the sensor appliance and the NSM Subsystem. An Update Server subsystem is also available, but since it is neither delivered to nor operated by the TOE users, it is outside the TOE boundary. Each subsystem performs dedicated functions.

[2] Artemis functionality is only available using M-Series sensors.

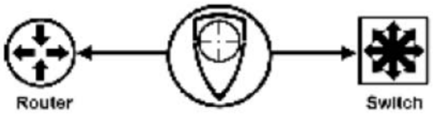
1.10 TOE Components

1.10.1 Collection Subsystem

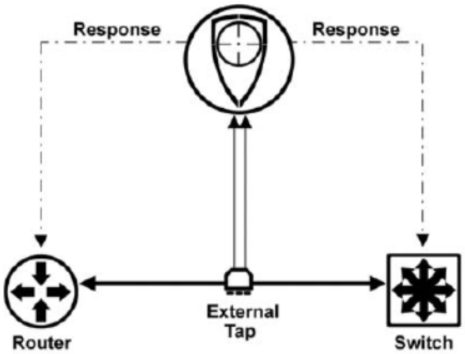
The Collection Subsystem is provided by the NSP sensor appliance. The primary function of the NSP sensor is to analyze traffic on selected network segments and to respond when an attack is detected. The sensor examines the header and data portion of every network packet; scanning for patterns and behavior in the network traffic that indicates malicious activity.

The sensor can operate in three modes:

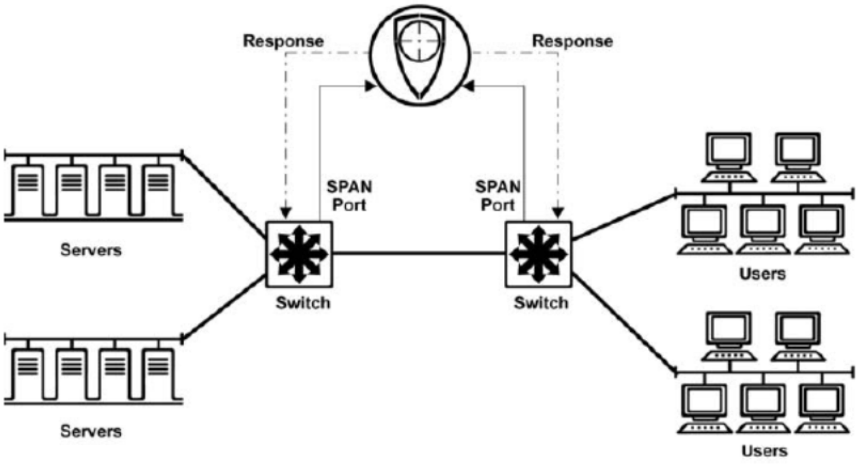
- Inline: The product is installed as an appliance within the network that applicable traffic must flow through.



- Tap: The network traffic flows between the clients and servers and the data is copied by the tap to the sensor which is essentially invisible to the other network entities. Note that the TOE cannot inject response packets back through an external tap, so NSP sensors offer Response ports through which a response packet (such as a TCP reset) can be injected to close a malicious connection.



- Span: The traffic is *spanned* off either the server side or the client side of a router or switch, copying both the incoming and outgoing traffic from any one of the ports. This requires a special network device that has a span port capability. Note that SPAN mode is also a “sniffing” mode, which—unlike inline mode—does not enable the TOE to prevent attacks from reaching their targets. However, while the TOE can issue response packets via the sensor’s response ports, some switches allow response packets to be injected by an IPS back through the SPAN port.



A single multi-port NSP sensor can monitor many network segments in any combination of *operating modes*; *monitoring* or *deployment* mode for the sensor; SPAN mode, TAP mode, or IN-LINE mode.

The NSP's Virtual IDS (VIDS) feature enables you to further segment a port on a sensor into many "virtual sensors". A VIDS can be *dedicated* to a specific network port with monitoring rules appropriate for that segment which might be different than the rules used to monitor other segments. Alternately, if a monitored network segment includes the use of Virtual LANs (VLANs) or Classless Inter-Domain Routing (CIDR); one or more VIDS can be directed at monitoring them with VIDS each configured with distinct monitoring rules. Note that VIDS are not particularly security relevant in and of themselves, but rather serve to organize and distinguish monitoring rules.

1.10.2 Manager Subsystem

The NSM is the Manager Subsystem and includes the software for the console platform. The NSM is a dedicated Windows Server 2008 platform running the NSM software. The NSM is also referred to as "The Manager". There are three versions of the NSM and all offer the same functionality:

1. *NSM Global Manager* supports unlimited number of sensors and is best suited for global IDS deployments.
2. *NSM Standard Manager* that supports deployments of up to six sensors.
3. *NSM Starter Manager* that supports up to 2 sensors.

The NSM software includes a Web-based user interface for configuring and managing the NSP Sensors.

The NSM includes the following components:

- *Home Page;* Is the first screen displayed after the user logs on to the system. The Home Page displays system health—i.e., whether all components of the system are functioning properly, the number of unacknowledged alerts in the system and the configuration options available to the current user. Options available within the Network Console are determined by the current user's assigned role(s).

- *System Health Viewer:* Displays the status of the NSM, database, and any deployed sensors, including all system faults.
- *System Configuration Tool:* Provides all system configuration options, and facilitates the configuration of sensors, administrative domains, users, roles, attack policies and responses, user-created signatures, and system reports. Access to various activities, such as user management, system configuration, or policy management is based on the current user's role(s) and privileges.
- *Reporting Component:* Reporting component within the Client application JSP which includes the home page, system health viewer, system configuration tool and reporting functions.
- *Threat Analyzer:* Displays detected security events that violate your configured security policies. The Threat Analyzer provides powerful drill-down capabilities to enable you to see all the details on a particular alert, including its type, source and destination addresses. The Threat Analyzer is deployed as part of the Thick Client.
- *UDS Editor:* User Defined Signature (UDS) editor allows customers to define custom user defined signatures. Similar to the Threat Analyzer, it is a thick client running on the client machine in the operational environment.

Access to the NSM is solely via the Console Machine for the CC Evaluated Configuration.

1.11 Operational Environment

1.11.1 Network Access

The TOE requires network access to the following support mechanisms in the Operational Environment (outside of the management network):

1. McAfee Update Server
2. OCSP server to support certificate revocation checking.
3. DNS server to support Artemis lookups.
4. SMTP server (optional)

No other connections are allowed outside of the management network.

1.11.2 Management

Local network access must be allowed to the following resources:

1. Console Workstation running Windows XP with Internet Explorer 7 or later with a CAC reader attached.
2. SNMPv3 client (optional)
3. Syslog server (optional)

1.12 Software/Hardware Components

The TOE consists of software developed by McAfee and 3rd party developers and hardware developed by 3rd party manufacturers.

Component	Version	Part of the TOE
NSP Sensor Software Installed on McAfee hardware platform	I-Series – 6.1.1.7 M-Series – 6.1.15.35	Yes
Network Security Manager software Installed on NSM platform	6.1.15.17	Yes
Network Security Manager platform • Platform running Windows Server 2008 SP1		No
Windows Server 2008 SP1 Underlying Operating system installed on NSM hardware platform to support NSM software		No
Windows XP with Internet Explorer 7 or later		No
Console workstation hardware platform Console Platform supporting Microsoft Internet Explorer browser interface used for accessing NSM		No
Common Access Card (CAC) software drivers Installed on the NSM console workstation		No
Common Access Card (CAC) reader hardware Installed on the Console workstation.		No
SSL Certificates (private keys) of traffic intended to be decrypted by the TOE		No

1.13 TOE Guidance Documentation

The following guidance documents are provided for download with the TOE software in accordance with EAL 2 requirements from the McAfee support website and apply to the CC Evaluated configuration:

1.14 System level guides

1. Getting Started Guide revision 5.0 McAfee® Network Security Platform Version 6.0 700-2365-00/ 4.0
2. Release Notes – Network Security Platform 700-2360E00
3. IPS Configuration Guide revision 1.0 McAfee® Network Security Platform version 6.0 700-2372-00/ 1.0
4. IPS Deployment Guide revision 2.0 McAfee® Network Security Platform version 6.0 700-2366-00/ 2.0
5. System Status Monitoring Guide Revision 3.0 McAfee® Network Security Platform Network Security Manager version 6.0 700-2375-00/ 3.0
6. Network Security Platform (NSP) Common Criteria Supplement EAL2 + ALC_FLR.2 Document Version 1.1

1.15 Applicable Sensor Quick Start Guides

1. Network Security Platform® M-6050 Quick Start Guide 700-2398-00
2. Network Security Platform® M-8000 Quick Start Guide 700-2400-00
3. Network Security Platform M-1250/M-1450 Quick Start Guide 700-2396-00
4. Network Security Platform M-2750 Quick Start Guide 700-2392-00
5. Network Security Platform M-2850/M-2950 Quick Start Guide 700-2651C00
6. Network Security Platform® M-3050/M-4050 Quick Start Guide 700-2394-00
7. Intrushield I-2700 Quick Start Guide 700-1063-03-G
8. Intrushield I-4010, I-3000 Quick Start Guide 2.1 700-1013-03-G
9. Intrushield I-4000 Quick Start Guide 2.1 700-1261-00-G
10. Intrushield I-1200, I-1400 Quick Start Guide 2.1 700-1259-00-revB

1.16 Applicable Product Guides

1. Administrative Domain Configuration Guide revision 3.0 McAfee® Network Security Platform Network Security Manager version 6.0 700-2368-00/ 3.0
2. Best Practices Guide revision 6.0 McAfee® Network Security Platform Network Security Manager version 6.0 700-2379-00/ 6.0

3. Manager Configuration Basics Guide revision 2.0 McAfee® Network Security Platform Network Security Manager version 6.0 700-2367-00/ 2.0
4. Reports Guide revision 3.0 McAfee® Network Security Platform Network Security Manager version 6.0 700-2376-00/ 3.0
5. Special Topics Guide - Virtualization revision 1.0 McAfee® Network Security Platform Network Security Manager version 6.0 700-2383-00/ 1.0
6. Troubleshooting Guide revision 5.0 McAfee® Network Security Platform Network Security Manager version 6.0 700-2380-00/ 5.0
7. Custom Attack Definitions Guide revision 1.0 McAfee® Network Security Platform Network Security Manager version 6.0 700-2377-00/ 1.0
8. M-1250/M-1450 Sensor Product Guide revision 2.0 700-2395-00/ 2.0
9. M-2750 Sensor Product Guide revision 3.0 700-2391-00/ 3.0
10. M-2850/M-2950 Sensor Product Guide revision 1.0 700-2652-00 1.0
11. M-3050/M-4050 Sensor Product Guide revision 2.0 700-2393-00/ 2.0
12. M-6050 Sensor Product Guide revision 2.0 700-2397-00/ 2.0
13. M-8000 Sensor Product Guide revision 2.0 700-2399-00-G/ 2.0
14. NSP Sensor I-4010 Product Guide revision 2.0 700-2390-00/ 2.0
15. NSP Sensor I-4000 Product Guide revision 1.0 700-2389-00/ 1.0
16. NSP Sensor I-3000 Product Guide revision 2.0 700-2388-00/ 2.0
17. NSP Sensor I-2700 Product Guide revision 1.0 700-2387-00/ 1.0
18. NSP Sensor I-1400 Product Guide revision 2.0 700-2386-00/2.0
19. NSP Sensor I-1200 Product Guide revision 2.0 700-2385-00/ 2.0
20. CLI Guide Revision 2.0 McAfee® Network Security Platform Network Security Manager version 6.0 700-2370-00/ 2.0
21. Device Configuration Guide Revision 4.0 McAfee® Network Security Platform Network Security Manager version 6.0 700-2371-00/ 4.0
22. Installation Guide revision 5.0 McAfee® Network Security Platform Network Security Manager version 6.0 700-2252-00/ 5.0
23. Manager Server Configuration Guide revision 2.0 McAfee® Network Security Platform Network Security Manager version 6.0 700-2369-00/ 2.0
24. Addendum I to 6.0 Documentation revision 1.0 McAfee® Network Security Platform version 6.0 / 700-2501-00/ 1.0
25. Addendum II to 6.0 Documentation revision 1.0 McAfee® Network Security Platform version 6.0 / 700-2509-00/ 2.0
26. Addendum III to 6.1 Documentation revision 1.0 McAfee® Network Security Platform version 6.0 / 700-2655-00 / 1.0

27. Integration Guide revision 4.0 McAfee® Network Security Platform version 6.0 / 700-2374-00 / 4.0
28. Network Security Platform FIPS Label Placement Procedure (Applicable for M-1450 and M-1250) 700-2272-00-revA
29. Network Security Platform FIPS Label Placement Procedure (Applicable for M-2750) 700-2346-00-revA (Note: This applies to the M-2850 and M-2950 in addition to the M-2750)
30. Network Security Platform FIPS Label Placement Procedure (Applicable for M-3050) 700-2271-00-revA
31. Network Security Platform FIPS Label Placement Procedure (Applicable for M-6050 and M-4050) 700-2270-00-revA
32. Network Security Platform FIPS Label Placement Procedure (Applicable for M-8000) 700-2356-00-revA

1.17 Logical Boundaries

The logical boundaries of the TOE include those security functions implemented exclusively by the TOE.

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TSF
- Cryptographic Operations
- System Data Collection
- System Data Analysis
- System Data Review, Availability, and Loss

The logical boundaries of the TOE are divided into two broad groups, one related to the administration and security attributes associated with the TOE; Security Audit, Identification and Authentication, Security Management, Cryptographic Operations and Protection of the TOE Security Functions and the other related to the collection and analysis of the network traffic (System Data Collection, Data Analysis and Data Review, Availability, and Loss).

1.17.1 Security Audit

The NSP system generates audit records related to the administration and management of the TOE and traffic logs for IDS information using the NSM component. The NSM management platform records both the audit and traffic log information into a data store in MySQL which is part of the TOE.

Auditable actions include changes to the IDS rules and viewing the audit records of both the system access and the IDS traffic log.

The NSP Sensor generates audit records relating to Sensor operation and forwards these logs to the NSM for integration and storage. This includes IDS related events local to the Sensor.

Only Authenticated users holding the Audit Administrator role can view audit records.

1.17.2 Identification and Authentication

The NSM provides an external user interface access which requires users to provide unique identification and authentication credentials using Common Access Cards before any access to the TOE services is granted.

NSM is compatible with Common Access Card (CAC) authentication systems that are used in conjunction with the NSM browser client installed on the console machine. The NSM does not support the ability to manage certificate revocation internally and depends on the OCSP server in the Operational Environment for this function.

The Sensor component is authenticated by the NSM component through a shared secret that is configured during the initial installation and setup process.

1.17.3 Security Management

The NSM provides a web-based (using https) management interface for all administration, including the IDS rule set, user accounts and roles, and audit functions. This GUI based interface allows for TOE configuration and Intrusion Protection System (IPS) management including Policies, Access Control Lists (ACL), Cryptographic settings, Alert and Quarantine Management, and Database Management/Archiving Utilities.

The Network Security Manager management interface is accessed using the Console machine. The thick client component, running within a browser session, provides a GUI interface to the NSM and allows management of the NSP system. This client component also includes the Threat Analyzer (TA) application and the User Defined Signature (UDS) editor that allows the creation of threat signatures by administrative users. These sessions are secured using TLSv1.0.

SNMPv3 is supported for NSM monitoring of deployed NSP sensors in the deployed environment by the NSM. These sessions are authenticated using a shared secret.

1.17.4 Protection of TSF

The TOE users must authenticate to the TOE before any administrative operations can be performed on the system.

The MIB configuration between the NSM and the sensor is implemented via SNMPv3. The AES encrypted data (signature and profile files) transferred between the NSM and NSP sensor(s) implements a TLSv1 session.

The data (signature files) communicated between the Update Server and the NSM is encrypted using TLS Version 1.0 to ensure confidentiality while in transit.

The NSP sensors components presence on the network is transparent. The NSP system is protected from the monitored networks as the system is configured to not accept any management requests or input.

The NSM management component is installed on a dedicated Windows Server 2008 platform running the NSM software.

All MySQL Database tables used for IDS system data are dynamically allocated so that the limit on the recording capacity of the collected information is the limit of the physical disk partition on the platform that is not dedicated to the operating system, the MySQL Database, and the Network Security Manager (NSM). This assures there is always adequate disk space to record current and new data that has been found to match the current rule set. However, as a safety feature, if the IDS system data could not be written to a MySQL Database table, an alarm is presented at the NSM console.

Audit records have an allocated 50,000 row table within the MySQL database that allows for storage of audit records in a circular buffer type arrangement. In the event the allocated rows are exhausted, the older audit records are overwritten and an alarm is presented at the NSM console. A new alarm is presented upon the initial overwrite.

The TOE depends on the underlying Operating System of the NSM component to provide reliable timestamps. The TOE ensures consistent timestamps are used by sharing that time information with its associated NSP sensors, so that all parts of the TOE share the same relative time information.

The MySQL Database within NSM can only be accessed through the local host and is further protected by a separate username and password configured during installation and stored in an obfuscated form within the NSM configuration. MySQL is accessible only to the NSM application within the evaluated configuration.

1.17.5 Cryptographic Operations

Cryptographic services are used by the NSP TOE for securing Console to NSM sessions, NSM to Sensor sessions and McAfee Update server to NSM sessions using encryption.

All M-series sensors are FIPS 140-2 validated (FIPS 140-2 Certs. #1646, #1653, and #1665).

The cryptographic modules within the NSP Sensors support the following algorithms. The M-Series FIPS algorithm certificates are also listed:

- AES CBC mode with 128 or 256 bits for encryption and decryption (Cert. #880) – TLSv1.0
- RSA with 1024 and 2048 bit keys for signature generation/verification (Cert. #425 & 830) – TLS
- SHA-1 for hashing (Cert. #871)
- ANSI X9.31 RNG (Cert. #505) with 2-Key Triple-DES ECB (Cert. #781) – TLS
- XYSSL RSA with 2048 bit keys for image verify (Cert. #830)
- XYSSL SHA-1 for hashing (Cert. #871)

In FIPS mode, the NSM Application cryptographic module within the NSM Component of the TOE supports the following FIPS approved algorithms based on the referenced certificates:

- BSafe TLSv1: AES – 128 bits CBC and CFB (Cert. #1237)
- BSafe TLSv1: RSA Verify 1024 bits (Cert. #593)
- BSafe TLSv1 and elsewhere: SHA-1 (Cert. #1135)

- BSafe TLSv1 and elsewhere: RNG FIPS 186-2 –SHA-1 G function. (Cert. #684)
- BSafe TLSv1 and elsewhere: HMAC SHA-1 (Cert. #721)

In FIPS mode, the NSM User Interface cryptographic module within the NSM Component of the TOE supports the following FIPS approved algorithms based on the referenced certificates:

- Open SSL TLSv1: AES 128 and 256 CBC mode (Cert. #1238)
- Open SSL TLSv1: TDES 128 (Cert. #886)
- Open SSL TLSv1: HMAC - SHA-1 (Cert. #721)
- Open SSL TLSv1: SHA-1 (Cert. #1135 & 1136)
- Open SSL TLSv1: RSA Sign/Verify 1024, 2048 (Cert. #594)
- Open SSL TLSv1 and elsewhere: RNG ANSI X9.31 (Cert. #685)
- BSAFE: HMAC-SHA-1 (Cert. #721)
- BSAFE: SHA-1 (Cert. #1135)

The TOE uses the following FIPS allowed algorithms and protocols:

- RSA with 1024 bit keys for key wrap decryption only (of bulk channel encryption/decryption key) – key wrapping; key establishment methodology provides 80 bits of encryption strength
- NDRNG for seeding the ANSI X9.31 RNG
- TLS v1.0 (with algorithm tested ciphers)

All sessions between TSF components and with the McAfee Update Server in the Operational Environment are conducted over encrypted channels using TLS v1.0. All sessions are symmetrically encrypted using the AES algorithm with 128 bit keys.

1.17.6 System Data Collection

The TOE has the ability to set rules to govern the collection of data regarding potential intrusions. The signature updates available on the Update Server contain default rules to detect currently known vulnerabilities and exploits and new rules can be created and/or imported to detect new vulnerabilities as well as specific network traffic.

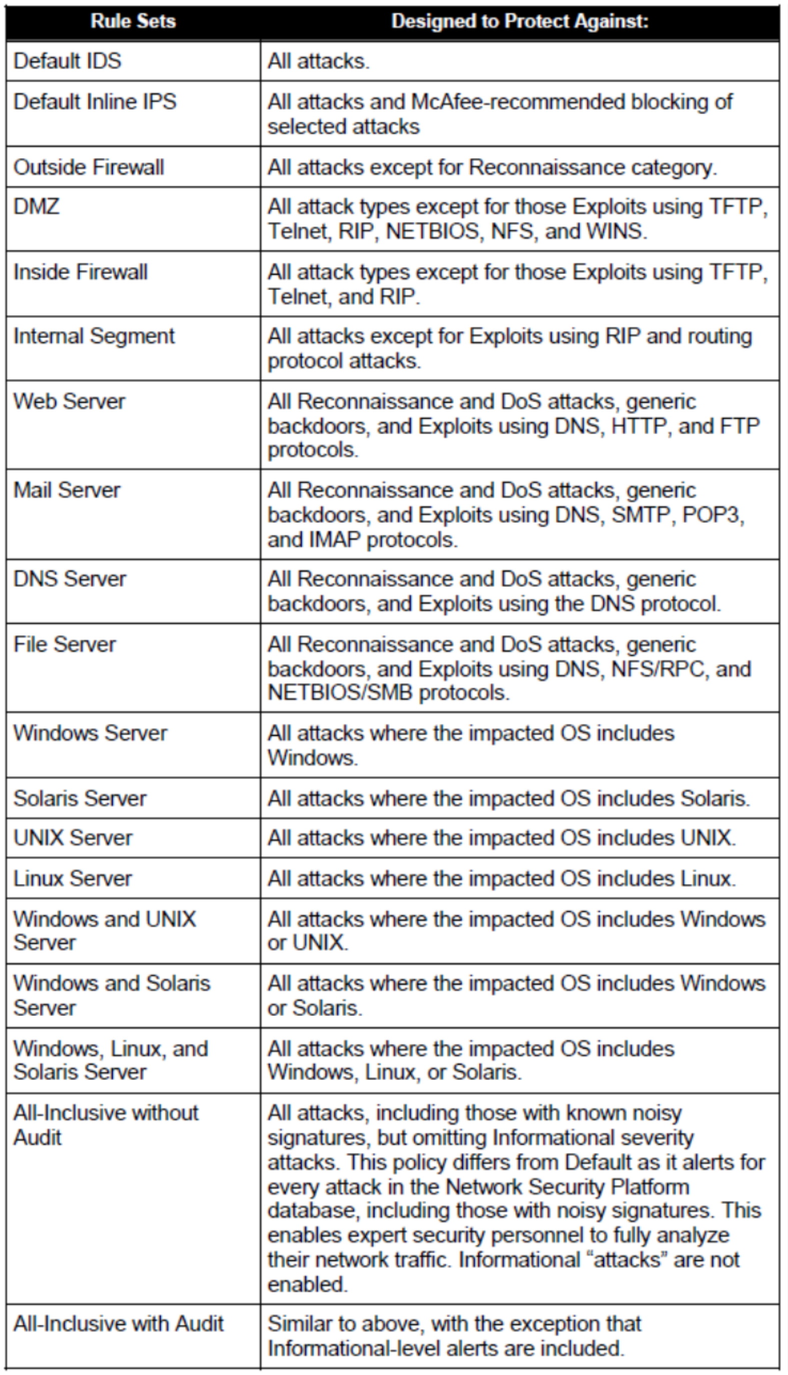
The TOE provides pre-configured rule sets and policies for immediate application in a number of different network areas. Each pre-configured policy is matched with an identically named rule set designed to address the common attacks targeting specific network environments. Existing rule sets cannot be modified but they may be “cloned” and then modified to create a custom rule set.

Attacks coverage by rule sets are managed by the following categories:

- Denial of Service (DoS), including DDoS
- Exploit
- Policy Violation

- Reconnaissance

The following pre-configured rule sets are included:



Rule Sets	Designed to Protect Against:
Default IDS	All attacks.
Default Inline IPS	All attacks and McAfee-recommended blocking of selected attacks
Outside Firewall	All attacks except for Reconnaissance category.
DMZ	All attack types except for those Exploits using TFTP, Telnet, RIP, NETBIOS, NFS, and WINS.
Inside Firewall	All attack types except for those Exploits using TFTP, Telnet, and RIP.
Internal Segment	All attacks except for Exploits using RIP and routing protocol attacks.
Web Server	All Reconnaissance and DoS attacks, generic backdoors, and Exploits using DNS, HTTP, and FTP protocols.
Mail Server	All Reconnaissance and DoS attacks, generic backdoors, and Exploits using DNS, SMTP, POP3, and IMAP protocols.
DNS Server	All Reconnaissance and DoS attacks, generic backdoors, and Exploits using the DNS protocol.
File Server	All Reconnaissance and DoS attacks, generic backdoors, and Exploits using DNS, NFS/RPC, and NETBIOS/SMB protocols.
Windows Server	All attacks where the impacted OS includes Windows.
Solaris Server	All attacks where the impacted OS includes Solaris.
UNIX Server	All attacks where the impacted OS includes UNIX.
Linux Server	All attacks where the impacted OS includes Linux.
Windows and UNIX Server	All attacks where the impacted OS includes Windows or UNIX.
Windows and Solaris Server	All attacks where the impacted OS includes Windows or Solaris.
Windows, Linux, and Solaris Server	All attacks where the impacted OS includes Windows, Linux, or Solaris.
All-Inclusive without Audit	All attacks, including those with known noisy signatures, but omitting Informational severity attacks. This policy differs from Default as it alerts for every attack in the Network Security Platform database, including those with noisy signatures. This enables expert security personnel to fully analyze their network traffic. Informational "attacks" are not enabled.
All-Inclusive with Audit	Similar to above, with the exception that Informational-level alerts are included.

Figure 1: Default Rule Sets

1.17.7 User Data Protection

The TOE offers mechanisms to import custom, user created or supplied data. The TOE protects the use and transfer of this data throughout transit, and in use. All communications are dune using secure channels and require authentication prior to allowing any information to be transferred into the TOE.

1.17.8 System Data Analysis

The TOE provides tools at the NSM console for menu selection to analyze both IDS traffic log data and audit logs. The TOE provides two methods of reviewing traffic log information; a real-time viewer at the NSM console and Audit information is reviewed from the console through the user Activities Audit Report.

Data Analysis is conducted using threat signatures that contain characteristics known to be representative of malicious traffic, malware, virus or worm infections. A series of threat signatures are provided and regularly updated to allow the NSP TOE to identify potentially malicious traffic. A second mechanism, the User Defined Signature (UDS) feature allows Security Administrator users to develop custom signatures and use them for traffic analysis.

The Threat Analyzer on the NSM console, allows the Security Administrator to perform analysis on alerts generated by NSP Sensors.

Report Generation

The TOE allows administrative users holding the Security Administrator role to generate a range of reports for both the alert information reported to the NSM and information pertaining to the Network Security Platform configuration settings.

1.17.9 System Data Review, Availability and Loss

IDS Audit data can only be viewed by authorized users (specific role). The NSM console provides a user interface for menu selectable data review.

1.18 Roles

The TOE supports the following roles:

1. Security Administrator
2. Crypto Administrator
3. Audit Administrator

1.19 Features Excluded from the Common Criteria Evaluated Configuration

The following features are excluded from the Common Criteria Evaluated configuration and therefore are not included in the evaluation:

1. Any update of TOE Software (other than threat signature updates)
2. Incident Generator
3. Sensor Failover Functionality; Sensor/Port Clustering (including associated interface groups)
4. Features associated with e-Policy Orchestrator Integration (Host Intrusion Prevention (HIP))
5. Features associated with McAfee Virus Scan (MVS) and FoundStone Integration. These are separate pieces of software not included with the TOE.
6. Network Access Control (NAC) features & integration with MNAC agents/server components
7. N-450 Sensor Appliance as this model pertains to the (excluded) NAC feature/deployment option

8. Multiple NSM configuration deployments: Manager Disaster Recovery (MDR), hierarchical NSM (Network Security Central Manager)
9. NSM: XML converter tool for ACL rules
10. Sensor Auxiliary Port
11. The Sensor CLI interface is excluded for use from the CC Evaluated configuration.
12. External Authentication server (LDAP/RADIUS/TACACS) and username/password based authentication to the NSM (CAC only allowed for CC Evaluated configuration)
13. Compact Flash Readers and/or PCMCIA/CardBus interfaces on Sensor Appliances (based on model)
14. Management of previous versions of sensors (6.1 NSM managing a 5.X sensor)
15. NTBA appliance Management
16. ePO integration
17. Password strength and account lockout features (CAC only prohibits this functionality)
18. M-Series SSL-decryption (this feature is not available to the user)

2 Conformance Claims

2.1 Common Criteria Conformance Claims

This Security Target is conformant to the Common Criteria Version 3.1r3, CC Part 3 conformant, CC Part 2 extended. The TOE is compliant with International Interpretations with effective dates on or before September 2010.

2.2 Conformance to Protection Profiles

This Security Target claims conformance with the U.S. Government Protection Profile Intrusion Detection Systems For Basic Robustness Environments, Version 1.7.

2.3 Conformance to Security Packages

This Security Target does not claim conformance to any security function requirements package, neither as package-conformant or package-augmented.

This Security Target is Evaluation Assurance Level 2 (EAL 2) augmented.

2.4 Threats and Security Objectives not applicable

The following Threats and Security objectives included in the applicable PP are not applicable to the TOE based on the following rationale:

2.4.1 Scanner not applicable

The following threats and security objectives were excluded since the TOE does not contain scanner component:

- T.SCNCFG
- T.SCNMLC
- T.SCNVUL
- O.IDSCAN

2.4.2 No Transfer of IDS data to non-TOE components

The following Security Objective is excluded from this Security Target:

O.EXPORT When any IDS component makes its data available to another IDS component; the TOE will ensure the confidentiality of the System data.

The TOE only provides this functionality between its own TOE components, therefore, no external IT products are necessary and this requirement is not applicable.

This requirement applies to the transfer of information between trusted products.

2.5 Added Assumptions

The following assumptions are additional to the referenced Protection Profile requirements:

A.NTRSRC

A.NTRSRC/OE.NTRSRC requires that an OCSP Server, McAfee Update Server, and a DNS server is provided in the Operational Environment for the purpose of verifying the revocation status of certificates on behalf of the TOE, updating signature sets, and query the Artemis database for malicious traffic. This provides an additional requirement on the environment from that of the PP, but does not reduce or otherwise affect the existing requirements placed on the TOE by the applicable PP.

2.6 Added Organizational Security Policies

The following OSPs were added to the ST.

P.SYSADMIN/OE.SYSADMIN

P.SYSADMIN/OE.SYSADMIN places a requirement on the deployment of the NSM platform to assure that only the Security Administrator user holds credentials allowing access to the underlying OS file system. This requirement simply adds additional deployment instructions to the PP requirement: A.LOCATE which requires that unauthorized access to the platform is prevented. In preventing access to unauthorized persons, the credentials established for the NSM platform in the Operational Environment limit the underlying OS access to a single, highly privileged role.

2.7 Security Functional Requirements

This Security Target includes all of the Security Functional Requirements from the PP, except those exclusively related to authenticating external IT products. Specifically:

- FPT_ITA.1 – This requirement is intended to specify how audit and System data are made available to external (trusted) IT products that would provide audit and data services. The TOE provides these functions internally and no external IT products are necessary, therefore this requirement is not applicable. This SFR is associated with the O.EXPORT exclusion above.

This requirement applies to the transfer of information between trusted products. There is no
such transfer with NSP. This requirement was replaced with FPT_ITT.1 of the transfer of
information between the TOE components.

Refinement

- FMT_MOF.1.1a – This requirement was refined to include the required administrative roles that have permissions to modify the behavior of the functions of System data collection, analysis and reaction. The permission is limited to an authorized administrator known as the Security Administrator.

Iterations

- FAU_STG.2.3 - This requirement is intended to satisfy the need for the TSF to ensure that all “already recorded” audit records will be maintained when failure, attack occurs and that “newly generated” audit records will be maintained when the storage exhaustion occurs.

Exclusions

- As included and refined within the referenced Protection Profile, the FIA_AFL.1.1 and FIA_AFL.1.2 security requirements were intended to detect attempts by untrusted external IT products to access the TOE. The TOE does not allow access to itself from external IT products; only authorized users may access the TOE. Therefore, this requirement is not applicable.

3 Security Problem Definition

The TOE is intended to be used either in environments in which, at most, sensitive, but unclassified information is processed. This section contains assumptions regarding the security environment and the intended usage of the TOE and threats on the TOE and the Operational Environment.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

A.NTRSRC An OCSP Server, McAfee Update Server, and a DNS server will be available in the Operational Environment.

3.2 TOE Threats

The threats discussed below are addressed by the McAfee NSP TOE. The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself.

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

T.EAVESDROP A malicious user or process may observe or modify TSF data transmitted between a separate part of the TOE or between the TOE and a trusted IT Entity.

3.3 IT System Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.4 Organizational Security Policies

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

P. SYSADMIN The NSM platform shall be configured such that only the Security Administrator user has access to the underlying Operating System file system.

4 SECURITY OBJECTIVES

This section describes the security objectives for the TOE and the TOE's operating Environment. The security objectives are divided between TOE Security Objectives and Security Objectives for the Operating Environment.

The following are the IT security objectives for the TOE:

O.CRYPTO The TOE shall provide cryptographic functions (i.e., encryption/decryption) to maintain the confidentiality and allow for detection of modification of TSF data that is transmitted between physically separated portions of the TOE, or between the TOE and trusted IT Entities.

O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.

O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

O.RESPON The TOE must respond appropriately to analytical conclusions.

O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.

O.ACCESS The TOE must display an advisory warning message upon startup and allow authorized users to access only appropriate TOE functions and data.

O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

O.OFLOWS The TOE must appropriately handle potential audit and System data storage overflows.

O.AUDITS The TOE must record audit records for data accesses and use of the System functions.

O.INTEGR The TOE must ensure the integrity of all audit and System data.

4.1 Security Objectives for the Environment

The following security objectives apply to the Operational Environment and are satisfied by technical means by Operational Environment hardware/software:

OE.AUDIT_PROTECTION The Operational Environment will provide the capability to protect audit information.

OE.TSF_PROTECTION The Operational Environment will provide the capability to protect TSF data in transit between distributed TOE components.

OE.AUDIT_SORT The Operational Environment will provide the capability to sort the audit information

OE.TIME The Operational Environment will provide reliable timestamps to the TOE.

OE.INTROP The TOE is interoperable with the IT System it monitors.

OE.NTRSRC The Operational Environment will provide an OCSP Server, McAfee Update Server, and a DNS server.

These non-IT security objectives, in addition to corresponding assumptions, are to be satisfied without imposing technical requirements on the TOE. These objectives are satisfied through the application of procedural or administrative measures:

OE.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

OE.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

OE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.

OE.SYSADMIN The TOE must be configured such that only the Security Administrator users hold credentials necessary to access the underlying Operating System file system on the NSM platform.

4.2 Mapping of Security Environment to Security Objectives

The following table represents a mapping of the threats to the security objectives defined in this ST.

	O.CRYPTO	O.PROTCT	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	OE.INSTAL	OE.PHYCAL	OE.NTRSRC	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.AUDIT_SORT	OE.AUDIT_PROTECTION	OE.TSF_PROTECTION	OE.SYSADMIN
A.ACCESS																	X					
A.DYNMIC																X	X					
A.ASCOPE																	X					
A.PROTCT													X									
A.LOCATE													X									
A.MANAGE																X						
A.NOEVIL												X	X		X							
A.NOTRUST													X		X							
A.NTRSRC														X								
T.EAVESDR OP	X																					
T.COMINT		X					X	X			X											
T.COMDIS		X					X	X														
T.LOSSOF		X					X	X			X											
T.NOHALT			X	X			X	X														
T.PRIVIL		X					X	X														
T.IMPCON						X	X	X				X										
T.INFLUX									X													
T.FACCNT										X												
T.FALACT					X																	
T.FALREC				X																		
T.FALASC				X																		
T.MISUSE			X																			
T.INADVE			X																			
T.MISACT			X																			
P.DETECT			X							X								X				
P.ANALYZ				X																		
P.MANAGE		X				X	X	X				X			X	X						
P.ACCESS		X					X	X												X		
P.ACCACT								X		X								X	X			
P.SYSADMI N																						X
P.INTGTY											X											
P.PROTCT									X				X								X	
T.MISUSE			X																			

Table 1: Summary of Mappings between Threats and IT Security

4.3 Rationale for IT SECURITY OBJECTIVES

T.EAVESDROP A malicious user or process may observe or modify TSF data transmitted between separate part of the TOE or between the TOE and a trusted IT Entity.

O.CRYPTO mitigates this threat by providing for the use of cryptographic functions to detect when information has been modified.

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data and providing an advisory message upon session startup. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System’s collection and analysis functions by halting execution of the TOE.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

The O.AUDITS and O.IDSENS objectives address this policy by requiring collection of audit, Sensor, and Scanner data.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

The O.IDANLZ objective requires analytical processes are applied to data collected from Sensors and Scanners.

P.MANAGE The TOE shall only be managed by authorized users.

The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this policy by providing TOE self-protection.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

The O.INTEGR objective ensures the protection of data from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.TSF_PROTECTION objective protects TSF data in transit between distributed TOE components.

P. SYSADMIN The NSM platform shall be configured such that only the Security Administrator user has access to the underlying Operating System file system.

The OE.SYSADMIN objective ensures the proper access control mechanisms are in place to protect the underlying Operating System files.

4.4 Rationale for Assumption Coverage

This section provides a justification that for each assumption and the security objectives for the environment which cover that assumption.

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

The OE.INTROP objective ensures the TOE has the needed access.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will be managed appropriately.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

The OE.PHYCAL provides for the physical Protection of the TSF hardware and software.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

The OE.PHYCAL provides for the physical Protection of the TSF.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical Protection of the TSF by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NOTRST The TOE can only be accessed by authorized users.

The OE.PHYCAL objective provides for physical Protection of the TSF to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NTRSRC An OCSP Server, McAfee Update Server, and a DNS server will be available in the Operational Environment.

The OE.NTRSRC security objective requires that an OCSP Server, McAfee Update Server, and a DNS server is provided in the Operational Environment.

5 Extended Components Definition

The Extended Component Classes/Families used in this ST are from the Extended Components Requirements contained in the applicable Protection Profile in order to conform to Common Criteria 3.1 R3 requirements.

6 Security Requirements

The security requirements that are levied on the TOE are specified in this section of the ST. These security requirements are defined in Sections 6.2

6.1 Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify these operations.

Assignment:	**indicated with bold text**
Selection:	indicated with underlined text
Refinement:	***additions indicated with bold text and italics***
	deletions indicated with strike-through ~~bold text and italics~~
Iteration:	indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

The explicitly stated requirements claimed in this ST are denoted by the IDS class prefix in the unique short name for the explicit security requirement.

TOE Security Functional Requirements	
Audit	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.2	Guarantees of audit data availability
FAU_STG.4	Prevention of audit data loss
Cryptographic Operations	
FCS_CKM.1a	Cryptographic Key Generation - ***Symmetric Keys***
FCS_CKM.1b	Cryptographic Key Generation - ***Asymmetric Keys***
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1a	Cryptographic Operations - ***Console Sessions***

FCS_COP.1b	Cryptographic Operations- ***Update Server Sessions***
FCS_COP.1c	Cryptographic Operations - ***Sensor to NSM Management Platform sessions***
FCS_COP.1d	Cryptographic Operations **–** ***Hashing***
FCS_COP.1e	Cryptographic Operations - ***RSA Key Wrapping/Digital Signature verification***
FCS_COP.1f	Cryptographic Operations **–** ***SSL Decryption***
User Data Protection	
FDP_IFC.1	User Data Protection **–** ***User Data SFP***
FDP_IFF.1	Simple Security Attributes
FDP_ITC.1	Import of User Data (SSL Cert, SNORT signatures, Artemis signatures)
FDP_ITT.1	Transfer of User Data
Identification and Authentication	
FIA_UAU.1	Timing of authentication
FIA_ATD.1	User attribute definition
FIA_UID.1	Timing of identification
Security Management	
FMT_MOF.1a	Management of security functions behavior
FMT_MOF.1b	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static Value Initialization
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security roles
Protection of the TSF	
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITI.1	Inter-TSF detection of modification
FPT_ITT.1	Basic internal transfer protection
FPT_STM.1	Reliable Time Stamps
TOE Access	

FTA_TAB.1	Default TOE Access Banner
Intrusion Detection System (EXT)	
IDS_SDC.1	System Data Collection (EXT)
IDS_ANL.1	Analyser analysis (EXT)
IDS_RCT.1	Analyser react (EXT)
IDS_RDR.1	Restricted Data Review (EXT)
IDS_STG.1	Guarantee of System Data Availability (EXT)
IDS_STG.2	Prevention of System data loss (EXT)

Table 2: Functional Requirements

6.2 TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

6.2.1 SECURITY AUDIT (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) ***~~Start-up and shutdown of the audit functions~~***;*

b) All auditable events for the basic level of audit; and

c) **Access to the System and access to the TOE and System data.**

*The audit function cannot be started or shutdown

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, **the additional information specified in the Details column of Table 3: Audited Events**

Component	Event	Details
FAU_GEN.1	~~Startup and shutdown of audit functions~~	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	Object IDS, Requested access
FAU_SAR.1	Reading of information from the audit	

	records	
FAU_SAR.2	**Unsuccessful attempts to read information from the audit records**	
FAU_SEL.1	**All modifications to the audit configuration that occur while the audit collection functions are operating**	
FCS_CKM.1a, b	**Success/Failure of Key Generation function**	
FCS_COP.1a, b, c, d, e, f	**Success/Failure of the Cryptographic operation**	
FCS_CKM.4	**Zeroization of Cryptographic CSPs**	
FDP_IFF.1	**All decisions on requests for information flow.**	
FDP_ITC.1	**All attempts to import user data, including any security attributes**	
FDP_ITT.1	**All attempts to transfer user data, including the protection method used and any errors that occurred.**	
FIA_UAU. 1	**All use of the authentication mechanism**	**User identity, location**
FIA_UID.1	**All use of the user identification mechanism**	**User identity, location**
FMT_MSA.1	**All modifications of the values of security attributes**	
FMT_MOF.1a,b	**All modifications in the behavior of the functions of the TSF**	
FMT_MTD.1	**All modifications to the values of TSF data**	
FMT_SMF.1	**Use of the Management functions.**	
FMT_SMR.1	**Modifications to the group of users that are part of a role**	**User identity**
FPT_ITI.1	**Action taken upon detection of modification of transmitted TSF data.**	

Table 3: Audited Events

6.2.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **Audit Administrator** with the capability to read **all Audit data** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.3 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.1.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform **sorting** of audit data based on **date and time, subject identity, type of event, and success or failure of related event.**

6.2.1.5 FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type;

b) **threat signature type**

6.2.1.6 FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to prevent modifications to the audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that **all** stored audit records will be maintained when the following conditions occur: attack.

6.2.1.7 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall overwrite the oldest stored audit records and send an alarm if the audit trail is full.

6.2.2 Cryptographic Operations (FCS)

6.2.2.1 FCS_CKM.1a Cryptographic key generation – Symmetric Keys

FCS_CKM.1.1a The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **software DRNG** and specified cryptographic key **168 bits (TDES), 128 or 256 bits (AES)** that meet the following: **ANSI X9.31 (Sensor), FIPS 140-2. FIPS 186-2 (NSM)***

*provided by the OpenSSL cryptographic modules within the Sensor components and the OpenSSL and Bsafe cryptographic modules within the NSM.

6.2.2.2 FCS_CKM.1b Cryptographic key generation – Asymmetric Keys

FCS_CKM.1.1b The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm **software DRNG** and specified cryptographic key sizes **1024, 2048** that meet the following: **ANSI X9.31, FIPS 140-2.**

6.2.2.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The ***Sensor component of the*** TSF shall destroy cryptographic keys in accordance with a specified key destruction method **cryptographic key zeroization method** that meets the following: **The Key Zeroization Requirements in FIPS PUB 140-2 Key Management Security Level 2**

6.2.2.4 FCS_COP.1a Cryptographic operation – *Console Sessions*

FCS_COP.1.1a The TSF shall perform **encryption/decryption of NSM Console TLS Sessions** in accordance with a specified cryptographic algorithm **AES or TDES using RSA key exchange** and cryptographic key sizes **(AES) 128 or 256 bits; (TDES) 168 bits; 1024/2048 bits (RSA)** that meet the following: **FIPS 140-2**

6.2.2.5 FCS_COP.1b Cryptographic operation – Update Server Sessions

FCS_COP.1.1b The TSF shall perform **Update Server TLS based sessions** in accordance with a specified cryptographic algorithm **AES** and cryptographic key sizes **128 bits** that meet the following: **FIPS 140-2**

6.2.2.6 FCS_COP.1c Cryptographic operation: Sensor to NSM Management Platform sessions

FCS_COP.1.1c The TSF shall perform **encryption/decryption of NSP Sensor to NSM TLS sessions and SNMPv3** in accordance with a specified cryptographic algorithm **AES using RSA key exchange** and cryptographic key sizes **(AES) 128 bits; 1024/2048 bits (RSA)** that meet the following: **FIPS 140-2**

6.2.2.7 FCS_COP.1d Cryptographic operation: *Hashing*

FCS_COP.1.1d The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA1, MD5** and ~~***cryptographic key***~~ ***message digest*** sizes **160 bits SHA1, 128 bits MD5 t**hat meet the following: **FIPS 140-2 (SHA1), RFC 1321 (MD5).**

*SHA1 used for TLS integrity checking,

6.2.2.8 FCS_COP.1e Cryptographic operation – RSA Key Wrapping/Digital Signature Verification

FCS_COP.1.1e The TSF shall perform **RSA Key Wrapping/Digital Signature verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024, 2048 bits** that meet the following: **FIPS 140-2.**

6.2.2.9 FCS_COP.1f Cryptographic operation – SSL Decryption

FCS_COP.1.1f The TSF shall perform **decryption of monitored traffic** in accordance with a specified cryptographic algorithm **RC4, DES, TDES, AES** and cryptographic key sizes **56, 128, 168, 256 bits** that meet the following: **FIPS 46-3; FIPS 140-2; FIPS 197; Applied Cryptography (RC4).**

Application note: SSL-decryption does not apply to M-Series sensors, I-1200, or I-1400.

6.2.3 User Data Protection

6.2.3.1 FDP_IFC.1 User Data SFP

FDP_IFC.1.1 The TSF shall enforce the **User Data SFP** on **Certificates, Signatures**.

6.2.3.2 FDP_IFF.1 Simple Security attributes

FDP_IFF.1.1 The TSF shall enforce the **User Data SFP** based on the following types of subject and information security attributes: **Role, Data Classification (Certificate or Signature)**.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **user must be authorized per** Table 4: TSF Data/Operations by Access Role **for requested action.**

FDP_IFF.1.3 The TSF shall enforce the **no additional rules.**

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: **no additional rules.**

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **no additional rules**.

6.2.3.3 FDP_ITC.1 Import of User Data (SSL Cert, SNORT signatures, Artemis signatures)

FDP_ITC.1.1 The TSF shall enforce the **User Data SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none.**

6.2.3.4 FDP_ITT.1 Transfer of User Data

FDP_ITT.1.1 The TSF shall enforce the **User Data SFP** to prevent the modification of user data when it is transmitted between physically-separated parts of the TOE.

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **no action** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) User identity (Common Name);*

b) Authentication data (Trusted Certificate Authorities);*

c) Authorisations; and

d) none.

*Since the TOE supports only CAC based authentication, the user identity refers to the Common Name and the authentication data refers to the certificate trusted status.

6.2.4.3 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **no action** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.5 SECURITY MANAGEMENT (FMT)

6.2.5.1 FMT_MOF.1a Management of security functions behaviour

FMT_MOF.1.1a The TSF shall restrict the ability to modify the behaviour of the functions of **System data collection, analysis and reaction** to ~~authorised System administrators~~ **the Security Administrator.**

6.2.5.2 FMT_MOF.1b Management of security functions behaviour

FMT_MOF.1.1b The TSF shall restrict the ability to determine the behaviour of, disable, enable, modify the behaviour of **functions listed in Table 4** to **Roles defined in Table 4** .

6.2.5.3 FMT_MSA.1 Management of Security attributes

FMT_MSA.1.1 The TSF shall enforce **User Data SFP** to restrict the ability to query, modify, delete the security attributes **Signatures, Certificates,** to the **Security Administrator.**

6.2.5.4 FMT_MSA.3 Static Value Initialization

FMT_MSA.3.1 The TSF shall enforce the **User Data SFP** to provide permissive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the no roles to specify alternative initial values to override the default values when an object or information is created.

6.2.5.5 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **operations listed in Table 4** to **Roles defined in Table 4**.

TSF Data Access Privileges

	Security Administrator	Audit Administrator	Crypto Administrator
Audit Logs Read/Analyze		X	
Configure Audit Logs		X	
Configure Device List RW		X	
Configure Device List R	X		
Configure Manager RW	X		
Operational Status RW	X		
Reports IPS RW	X		
TA Summary Dashboard	X		
Configure Admin Domain RW	X		
User Creation RW	X		
Configure Guest Portal	X		
Configure Integration RW	X		
Configure IPS Settings RW	X		
TA Alerts RW	X		
TA Hosts RW	X		
Manually update NSM signatures	X		
Backup/restore audit records		X	
Configure Admin User Accounts R/W	X		
Configure Device List RO	X		
IPS RW	X		
IDS System Data R/W	X		
Sensor Configure Password policy settings R/W			X
Configure NSM banner RW	X		
Configure Sensor banner RW	X		
Import SSL Certificate	X		
Import Artemis Signatures	X		
Import custom MD5 Signatures	X		
Import SNORT signatures	X		

Table 4: TSF Data/Operations by Access Role

6.2.5.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

Audit Logs Read/Analyze

Configure Audit Logs
Configure Device List RW
Configure Device List R
Configure Manager RW
Operational Status RW
Reports IPS RW
TA Summary Dashboard
Configure Admin Domain RW
User Creation RW
Configure Guest Portal
Configure Integration RW
Configure IPS Settings RW
TA Alerts RW
TA Hosts RW
Manually update NSM signatures
Backup/restore audit records
Configure Admin User Accounts R/W
Configure Device List RO
IDS System Data R/W
Sensor Configure Password policy settings R/W
Configure NSM banner RW
Configure Sensor banner RW
Import SSL Certificate
Import Artemis Signatures
Import custom MD5 Signatures
Import SNORT signatures
Audit Logs Read/Analyze
Configure Audit Logs

6.2.5.7 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the **following roles**[3]**:**

- **Security Administrator**
- **Audit Administrator**
- **Crypto Administrator**

[3] Roles have been modified from the PP to meet UCAPL requirements

- ~~**authorised administrator**~~
- ~~**authorised System administrators**~~

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.6 PROTECTION OF THE TSF (FPT)

6.2.6.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

6.2.6.2 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: **a single failed integrity check.**

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform **resend affected packets** if modifications are detected.

6.2.6.3 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from modification when it is transmitted between separate parts of the TOE.

6.2.6.4 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

6.2.7 TOE Access (FTA)

6.2.7.1 FTA_TAB.1 Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.3 Extended TOE Security Functional Requirements

6.3.1 IDS COMPONENT REQUIREMENTS (IDS)

6.3.1.1 IDS_SDC.1 System Data Collection (EXT)

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) network traffic, detected known vulnerabilities; and

b) **No other events**.

IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) The additional information specified in the Details column of **Table 5: System Events**

Component	Event	Details
IDS_SDC.1	**Network traffic**	**Protocol, source address, destination address**
IDS_SDC.1	**Detected known vulnerabilities**	**Identification of known vulnerability**

Table 5: System Events

6.3.1.2 IDS_ANL.1 Analyser analysis (EXT)

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:

a) signature and

b) configured thresholds, statistical based anomaly, protocol anomaly-based detection (parameter length check), authorized administrator created rules/signatures

IDS_ANL.1.2 The System shall record within each analytical result at least the following information:

a) **Date and time of the result, type of result, identification of data source**; and

b) **none**

6.3.1.3 IDS_RCT.1 Analyser react (EXT)

IDS_RCT.1.1 The System shall send an alarm to **the administrator** and take **log an alert and perform one or more of the following:**

- **drop packet**
- **send TCP reset**
- **Quarantine the host (block)**
- **send ICMP host unreachable**
- **log packet**
- **Filter alert**

when an intrusion is detected.

6.3.1.4 IDS_RDR.1 Restricted Data Review (EXT)

IDS_RDR.1.1 The System shall provide **Security Administrator** with the capability to read **captured IDS data** from the System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

6.3.1.5 IDS_STG.1 Guarantee of System Data Availability (EXT)

IDS_STG.1.1 The System shall protect the stored System data from unauthorised deletion.

IDS_STG.1.2 The System shall protect the stored System data from modification.

IDS_STG.1.3 The System shall ensure that **all** System data will be maintained when the following conditions occur: failure, attack, System data storage exhaustion.

6.3.1.6 IDS_STG.2 Prevention of System data loss (EXT)

IDS_STG.2.1 The System shall overwrite oldest System data and send an alarm if the storage capacity has been reached.

6.4 Rationale for TOE Security Requirements

	O.CRYPTO	O.PROTCT	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	OE.TIME	OE.AUDIT_SORT	OE.AUDIT_PROTECTION
FAU_GEN.1										X				
FAU_SAR.1						X								
FAU_SAR.2							X	X						
FAU_SAR.3													X	
FAU_SEL.1						X								
FAU_STG.2		X					X	X	X		X			X
FAU_STG.4									X	X				
FIA_UAU.1							X	X						
FIA_ATD.1								X						
FIA_UID.1							X	X						
FCS_CKM.1a,b	X													
FCS_CKM.4	X													
FCS_COP.1a,b,c,d,e,f	X													
FDP_IFC.1					X									
FDP_IFF.1						X								
FDP_ITC.1		X												
FDP_ITT.1		X												
FMT_MOF.1a,b		X					X	X						
FMT_MSA.1						X								
FMT_MSA.3						X								
FMT_MTD.1		X				X	X	X			X			
FMT_SMF.1						X								
FMT_SMR.1								X						
FPT_ITC.1											X			
FPT_ITI.1											X			
FPT_ITT.1											X			
FTA_TAB.1							X							
FPT_STM.1										X		X		
IDS_SDC.1			X											
IDS_ANL.1				X										
IDS_RCT.1					X									
IDS_RDR.1						X	X	X						

	O.CRYPTO	O.PROTCT	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	OE.TIME	OE.AUDIT_SORT	OE.AUDIT_PROTECTION
IDS_STG.1		X					X	X	X		X			
IDS_STG.2											X			

Table 6: Summary of Mappings between Security Functions and IT Security Objectives

6.4.1 TOE Security Functional Requirements Rationale

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, Table 6: Summary of Mappings between Security Functions and IT Security Objectives illustrates the mapping between the security requirements and the security objectives and Table 1: Summary of Mappings between Threats and IT Security demonstrates the relationship between the threats, policies and IT security objectives. The functional and assurance requirements presented in this Security Target are mutually supportive and their combination meets the stated security objectives.

Security Objective	Mapping Rationale
O.CRYPTO	The TOE is required to protect TSF data from Eavesdropping when TSF data is sent between separate parts of the TOE or to a trusted IT Entity. FCS_CKM.1a is a requirement that a crypto module generate symmetric keys. Such keys are used by the AES/TDES encryption/decryption functionality specified in FCS_COP.1a, b, c. FCS_CKM.1b is a requirement that a crypto module generate asymmetric keys (public/private keypairs) for use in FCS_COP.1c FCS_COP.1a specifies that AES & TDES are used to perform encryption and decryption operations for TLS based sessions between the Console and the NSM TOE component. FCS_COP.1b requires that the TSF perform encryption/decryption of TLS sessions between the NSM and the McAfee Update Server in accordance with the referenced algorithms/standards. FCS_COP.1c requires that the TSF perform encryption/decryption of TLS sessions between the Sensor and the NSM TOE components in accordance with the referenced algorithms/standards. FCS_COP.1d requires that the TSF provide hashing services using a NIST-approved implementation of the Secure Hash Algorithm. FCS_COP.1e requires that the TSF provide RSA key wrap/unwrap services using the RSA algorithm and key sizes 1024, 2048 bits. FCS_COP.1f requires that the TSF perform encryption/decryption of TLS/SSL sessions flowing through the sensor and SNMPv3 communication in accordance with the referenced algorithms/standards. FCS_CKM.4 provides the functionality for ensuring key and key material is zeroized. This applies not only to key that resides in the TOE, but also to intermediate areas (physical memory, page files, memory dumps, etc.) where key may appear.

O.PROTCT	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1a, b]. Users can read, write or create TSF data based on the type of data and assigned role. [FMT_MTD.1]. All User data is protected from modification at time of importing [FDP_ITC.1] as well as when being transferred to other TOE components [FDP_ITT.1].
O.IDSENS	A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events must be defined in the ST [IDS_SDC.1].
O.IDANLZ	The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].
O.RESPON	The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1]. The TOE utilizes information received from environmental resources to correctly identify and analyze potential intrusions. [FDP_IFC.1]
O.EADMIN	The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SEL.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed. The system will provide mechanisms for the authorized administrator to react to threats observed in accordance with security policies. [FDP_IFF.1, FMT_MSA.1, FMT_SMF.1, FMT_MSA.3, FMT_MTD.1]
O.ACCESS	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2a, b]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1a, b]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1] The TOE presents an advisory message when starting a user session. [FTA_TAB.1]
O.IDAUTH	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1] The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1a, b]. Users can read, write or create TSF data based on the type of data and assigned role [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1].
O.OFLOWS	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack

	[FAU_STG.2]. The TOE must prevent the loss of audit data in the event its audit trail is full [FAU_STG.4]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The System must prevent the loss of audit data in the event the audit trail is full [IDS_STG.2].
O.AUDITS	Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU_SEL.1]. The TOE must prevent the loss of collected data in the event its audit trail is full [FAU_STG.4]. Time stamps associated with an audit record must be reliable [FPT_STM.1].
O.INTEGR	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Specified roles can read, write or create TSF data based on the type of data [FMT_MTD.1]. The TOE ignores all system data and sends an alarm when storage is at full capacity. [IDS_STG.2] The TOE encrypts and integrity checks TSF data sent from the McAfee update server to the TOE when receiving threat signature updates [FPT_ITC.1, FPT_ITI.1] and when transmitting between separate parts of the TOE. [FPT_ITT.1]
OE.TIME	The Operational Environment will provide reliable time stamps to the TOE and the TOE shall provide accurate time stamps to the application for use in audit records. Time stamps associated with an audit record must be reliable [FPT_STM.1].
OE.AUDIT_SORT	The Operational Environment must provide the ability to review and manage the audit trail of the System to include sorting the audit data [FAU_SAR.3].
OE.AUDIT_PROTECTION	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2].

6.5 Rationale For IT Security Requirement Dependencies

This section includes a table of all the security functional requirements and their dependencies and a rationale for any dependencies that are not satisfied.

Functional Component	**Dependency**	**Included/Rationale**
FAU_GEN.1	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_SAR.3	FAU_SAR.1	Yes
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	Yes
FAU_STG.2	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes, through FAU_STG.2
FCS_CKM.1a,b	FCS_CKM.4, FCS_COP.1	Yes, except FCS_CKM.4 not met for NSM
FCS_COP.1a,b,c,d,e,f	FCS_CKM.1a,b, FCS_CKM.4	Yes, except FCS_CKM.4 not met for NSM
FCS_CKM.4	FCS_CKM.1a,b	Yes
FDP_IFC.1	FDP_IFF.1	Yes
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	Yes
FDP_ITC.1	FDP_IFC.1, FMT_MSA.3	Yes
FDP_ITT.1	FDP_IFC.1, FDP_ACC.1	Yes
FIA_UAU.1	FIA_UID.1	Yes

Functional Component	Dependency	Included/Rationale
FIA_ATD.1	None	None
FIA_UID.1	None	None
FMT_MOF.1a,b	FMT_SMR.1, FMT_SMF.1	Yes
FMT_MSA.1	FDP_IFC.1, FMT_SMR.1, FMT_SMF.1	Yes
FMT_MSA.3	FDP_IFC.1, FMT_MSA.1, FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	Yes
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	Yes
FPT_ITC.1	None	None
FPT_ITI.1	None	None
FPT_ITT.1	None	None
FPT_STM.1	None	None
FTA_TAB.1	None	None
IDS_SDC.1	None	None
IDS_ANL.1	None	None
IDS_RCT.1	None	None
IDS_RDR.1	None	None
IDS_STG.1	None	None
IDS_STG.2	None	None

Table 7: SFR Dependencies

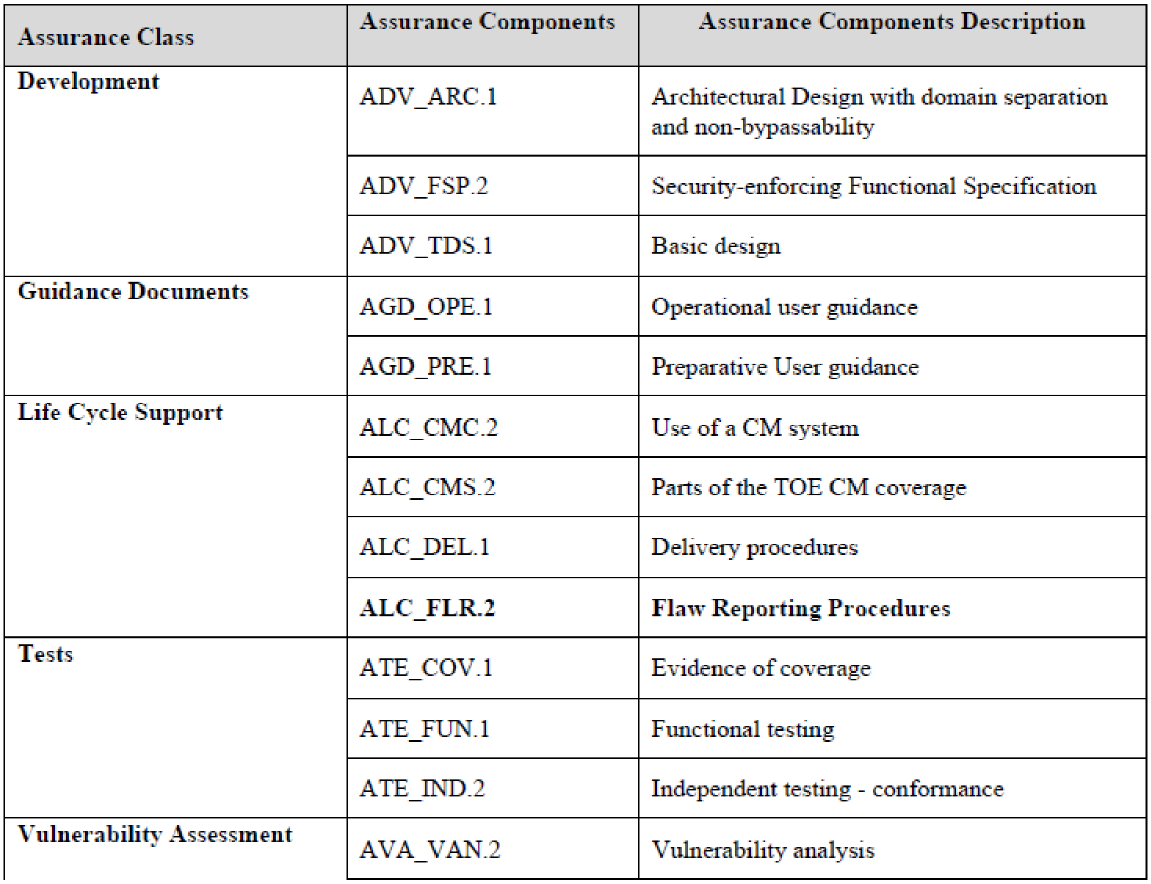
6.6 Rationale for TOE Dependencies Not Satisfied

The dependency for FCS_CKM.4 associated with FCS_CKM.1a, b is not satisfied on the NSM component of the TOE. Key material on this platform may be destroyed by "by uninstalling the application, formatting the hard drive and power cycling the device" as described in the following FIPS-140-2 Security Policy for the applicable NSM cryptographic module: *NSM Application Cryptographic Module Security Policy Version 1.2.*

6.7 TOE Security Assurance Requirements

EAL 2 + ALC_FLR.2 was chosen to provide a "basic" level of independently assured security. The chosen assurance level is consistent with the Protection Profile..

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 augmented (EAL 4 + ALC_FLR.2) as defined by the CC. The assurance components are summarized in the following table.



Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_ARC.1	Architectural Design with domain separation and non-bypassability
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	**Flaw Reporting Procedures**
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - conformance
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 8: Assurance Requirements: EAL 2 + ALC_FLR.2

7 TOE Summary Specification

The TOE's security functionality is characterized through the following Security Functions:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TSF
- User Data Protection
- Cryptographic Operations
- System Data Collection
- System Data Analysis
- System Data Review, Availability and Loss

7.1 Security Audit

FAU_GEN.1

The NSM management platform generates audit records for Console Administrative sessions and stores them into the MySQL database, running on the same dedicated platform as does the NSM management software. The MySQL Database provides storage and retrieval for audit log information. This function records attempts to access the system itself, such as successful and failed authentication and the actions taken by the user once authenticated. Auditable actions include changes to the IDS rules and viewing the audit records.

The NSP Sensor generates audit records based on Sensor detected events and forwards these logs to the NSM platform where they may be integrated into a single (NSP) log resource stored in the MySQL database.

The NSM records the audit information into a data store within the MySQL database. Events logged in audit records include the items listed in Table 3: Audited Events and are categorized by the following event types:

- Admin Domain Action
- User Action
- Manager Action
- Sensor Action
- Policy Action
- Report Action
- Update Server Action
- System Health Action

- Alert Action

The following information about an audited event is stored in the audit log whenever that audited event is recorded:

a) Date and time of the event,

b) Type (i.e., category and action) of event,

c) Subject (i.e., user and domain) identity,

d) Result (success or failure) of the event, and

e) Description (where applicable access mode, target object, etc.).

Actions that can be performed at the NSM Management Console are audited. This includes the following:

a) Access to the TOE and System data that includes the object ID's and the requested access (attempts to read the audit log, and alert acknowledgement and deletion);

b) All modification to the audit configuration that occur during collection (modification of audit settings);

c) All authentication attempts, including the user and location where authentication was attempted (all login attempts as well as user logoff events);

d) All modification to the behavior of the TSF (modification of audit settings, creation of policies, updating signatures)

e) All modifications to TSF data values (modification of audit settings, creation of policies, and updating signatures); and,

f) Modification of user accounts, creation, deletion, and modifications (create user, delete user, assign roles, and update roles).

g) Cryptographic Operations relating to establishing secure sessions between TOE components or the McAfee update server.

h) All decisions on requests for information flow.

i) All attempts to import user data, including any security attributes.All attempts to transfer user data, including the protection method used and any errors that occurred.

j) All modification to the values of security attributes.

k) Use of Management functions.

Audit records may be backed up in the form of a file through the NSM console. This invokes a MySQL database backup routine that places these records in a backup file on a storage resource. Files can also be restored to the NSM through the console using a database restore function.

Cryptographic functions within the NSM and Sensor components are audited including cryptographic operations, cryptographic key generation and destruction of cryptographic keys.

Review of Audit Records FAU_SAR.1

The NSM provides the ability for the authenticated users to view security audit data for the system. The TSF enforces that only the Audit Administrator has access to read information from the audit records. The audit logs are viewable through the standard web-based management interface provided by the NSM and accessed via the Console Browser client.

FAU_SAR.2 Restricted Audit Review

No security related actions can be taken without a successful user authentication therefore only authorized users who have been authenticated to a role with privileges of an authorized Audit administrator can view the audit records.

FAU_SAR.3 Selectable Audit Review

While viewing the security audit records from the NSM, it is possible to sort and filter the data based upon the following properties:

- Date and time
- User
- Type of event
- Success or failure of the event

FAU_SEL.1 Selectable Audit

The NSM allows a user with the Audit Administrator role to set the types of auditable events by their type. The NSM allows the Security Administrator to include or exclude auditable events from the set of audited events based on the event type.

A person assigned to the Audit Administrator role can include or exclude recorded events in the traffic log that match a specific signature.

FAU_STG.2 Guarantees of Data Availability

Access to audit records is available only via authenticated NSM console TLS sessions. The TOE provides protection for the security audit records primarily by TSF identification and authentication mechanisms. There are no TSF interface options available to disable audit or delete/modify audit records. The audit function starts automatically when the TOE is installed. Once recorded, audit data cannot be modified except, in the case where the audit log reach its capacity. Under these circumstances new audit data will overwrite the oldest audit data. This occurrence will also cause a system fault message to be posted to the system fault log. Only TSF interfaces to the audit mechanism allow for the creation of an audit log, viewing audit information, backing up and restoring audit log information.

The NSM relies on the underlying Windows Server 2008 operating system to protect the files as a storage repository for the TOE audit records.

FAU_STG.4 Prevention of Audit Data Loss

The data store within the NSM database allocates 50,000 rows for the purposes of storing audit records. In the event that the audit log storage resources are exhausted, an alarm is presented at the NSM console and the oldest data stored in the audit log is overwritten with the newest data.

7.2 Identification and Authentication

FIA_ATD.1 User Attribute Definition

User accounts in the TOE have the following attributes:

A X.509 certificate (derived from a CAC) that is passed to the NSM during the session negotiation process and, within that certificate, a Common Name that is extracted and checked against a user list on the NSM. The certificate also is required to be signed by a trusted CA as configured during NSP system setup.

User Identification and Authentication – FIA_UID.1, FIA_UAU.1

Identification and authentication is required for logical access to the NSM.

A Common Access Card (smartcard) with a valid digital certificate is required to establish a session with the NSM. NSM requests the certificate from the NSM browser client which invokes the necessary CAC software calls to extract the certificate from the smartcard. Once the certificate is obtained by the browser client, it is sent to NSM which verifies that the certificate is not revoked through the use of OCSP in the operation environment. If the certificate is verified to not be revoked, NSM parses the x.509 formatted certificate, extracts the Common Name and performs a lookup to verify the Common Name is included in the user database as holding a valid account. If successful, the user's session is initiated under the assigned role. If unsuccessful, the authentication attempt fails and connection is immediately terminated.

TOE Access Banners – FTA_TAB.1

The TOE NSM and Sensor components both present an advisory access banner prior to establishing a user session that may be configured to include a custom deployment specific warning about unauthorized access and use of resources and organizational graphics.

7.3 Security Management

The NSM provides a security management interface used to configure and manage the NSP TOE and provide a report and analysis utility for investigating traffic events.

The GUI based interface is divided into tabs based on the service available on respective pages of the display. The following tab categories are provided:

IPS Settings – Allows the configuration of IPS policies, Alert filters, Access Control Lists (ACL), Cryptographic settings, Quarantine configuration and Alert notifications

Summary – Provides a detailed view of all configured policies and their status

Policies – Provides a Policy Editor and Reconnaissance Policy editor for policy development, Policy Assignment section, HTTP response scanning settings.

Advanced Policies – Allows the configuration of policy rule sets, User Defined Signature editor

Alert Filters – Provides for Editing, Managing, Importing/Exporting Alert Filters

ACLs – Allows for viewing and management of Access Control Lists, including import/export options

IPS Quarantine – Allows configuration of IPS Quarantine within Policy Editors, Access Domains, IPS Sensors and Threat Analyzer.

Archiving – Supports Data Archive functions including auto archive scheduling

Maintenance – Provides an interface for Database management

Alert Notification – Allows the user to view/manage Alert settings

NSP Sensor SNMPv3 Interface

The NSP Sensor SNMPv3 interface facilitates the exchange of management information between itself and the NSM platform. Performance statistics, configuration data and management information can be queried through this interface for action by the appropriate user.

Communications between the NSM and the Sensor are sent via the secure channel using AES128-SHA1.

NSM SNMPv3 Interface

The NSM provides an SNMP interface for the purpose of reporting trap related information to devices in the Operational Environment. This interface is configured to be read-only for the CC Evaluated configuration. SNMPv3 traps are sent via AES128-SHA1.

FMT_MOF.1a, b - Management of Security Functions Behavior

Only authorized users can access any security functions on the system. Signatures files are updated by McAfee Incorporated on a protected server within a controlled space and/or by an administrative user with the Security Administrator role. Only users with Security Administrator role can:

- Implement rules on the NSP TOE.
- Create, delete, and modify existing rules on the system.
- Manage the security settings on the system, such as user accounts.

FMT_MTD.1, FMT_SMR.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, Management of TSF Data & Security Roles

The TSF is capable of maintaining the following roles: Security Administrator, Audit Administrator, Crypto Administrator.

The Authorized administrator role as defined in the applicable PP is also known within this ST as the Security Administrator role and the authorized System Administrator (PP reference) is also known as Security Administrator within this ST.

The following table describes the NSM roles supported for management of the NSP TOE and the applicable access level to data objects:

Role	General Description	Specific Read/Write Access
Security Administrator	NSM Full Access User: Security Administrators must manage themselves within the domain(s) they reside. They can read, modify, delete and push policy. Security Administrators can also administer other administrators and their roles, adding, maintaining, and deleting users and role assignments. Administers the Intrusion Prevention Environment	Configure Device List R Configure Manager RW Operational Status RW Reports IPS RW TA Summary Dashboard Configure Admin Domain RW User Creation RW Configure Guest Portal Configure Integration RW Configure IPS Settings RW TA Alerts RW TA Hosts RW

		Manually update NSM signatures Configure Admin User Accounts R/W Configure Device List RO IPS RW IDS System Data R/W Configure NSM banner RW Configure Sensor banner RW Import SSL Certificate Import Artemis Signatures Import custom MD5 Signatures Import SNORT signatures
Audit Administrator	Audit Administrator can read and analyze audit data, backup/restore audit data, and manage auditing facilities	Audit Logs Read/Analyze Backup/restore audit records
Crypto Administrator	Administer the Device List	Sensor Configure Password policy settings R/W Configure Device List RW

Table 9: NSM Access by Authenticated Role

7.4 Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

The NSP Sensors and NSM management platform all protect TSF data from disclosure and modification, when it is transmitted between separate parts of the TOE, by communicating using TLSv1 connections.

The Sensor communicates with the NSM management platform through its dedicated 10M/100M Ethernet port using TCP/IP. This communications uses secure channels; providing link privacy using encryption and mutual authentication using public key authentication. The ciphers suites used for this communications are TLSv1 (AES 128 SHA1).

FPT_ITC.1, FPT_ITI.1 TSF data confidentiality and integrity protection

Sessions between the McAfee Update Server and the NSM component of the TOE are secured using AES, 128 bit encryption over a TLS tunnel. Message integrity checking is provided by a SHA1 hash.

There is no communication between the sensor and Update Server.

FPT_STM.1 Reliable Time Stamps

The TOE uses Windows Time Services provided by the Windows Server 2008 operating system to provide time stamps for the TSF to write time stamps for audit records, both the security records and the System Data records. The NSM receives time stamps from the Windows Server 2008, which is part of the operational environment, ensuring they are reliable by consistently obtaining time information from the well-defined and presumed trusted and reliable source.

Each Sensor receives a time reference from the NSM management platform. The NSM management platform periodically passes a timestamp reference to the sensors. This occurs: On power up when establishing the crypto channels to NSM and upon every re-establishment due to link/network issues to NSM. Regardless, time is updated every 2 minutes post establishment.

Each Sensor uses this timestamp to synchronize its own independent timing mechanism synchronizing at regular intervals per the timestamps sent from the NSM management platform.

7.5 User Data Protection

FDP_IFC.1; FDP_IFF.1; FDP_ITC.1; FDP_ITT.1

The TOE does not allow access to any user data or management functions until after the user has been successfully authenticated. Access is only granted to the roles defined in Table 4: TSF Data/Operations by Access Role. All other users are not given access to the interfaces to allow user data import.

When data is being imported, it is protected at all times by the TLSv1 tunnel. This is true both for initial importing into the manager subsystem as well as upon transfer to the sensor subsystem at a later time (if so chosen).

7.6 Cryptographic Operations

FCS_COP.1a, b, c, d, e, f; FCS_CKM.4

The NSP system utilizes symmetric key cryptography to secure communications between TOE components and with the McAfee Update Server in the Operational Environment. All sessions, except SNMPv3, are conducted using TLSv1 and leverage an OpenSSL Module. Key exchange between the Console browser client and the NSM and the NSM and NSP Sensor is performed using RSA public/private key exchange. Cryptographic library support is provided for the NSM by an RSA BSafe cryptographic library and for the NSP Sensor by XySSL library. OpenSSL and both cryptographic libraries are contained within NSP software release packages. When TLS Administration sessions are closed, the OpenSSL module within the sensor component zeroizes all cryptographic keys used for the sessions.

SNMPv3 sessions are secured using the AES algorithm 128 bit key size.

Key Generation FCS_CKM.1a, b

Symmetric keys utilized for TLS connections are generated on demand using an OpenSSL based deterministic software random number generator (DRNG) using the TDES algorithm.

The NSM and NSP Sensor components generate asymmetric (public/private) keypairs using an OpenSSL based software RNG and the RSA algorithm of 1024/2048 bit key sizes.

The OpenSSL implementation used for the TOE utilizes a software based DRNG that is compliant with ANSI X9.31.

Console Sessions – FCS_COP.1a

Administrative User browser sessions between the NSM Console and the NSM Server platform are symmetrically encrypted using the AES or TDES algorithms and 128, 168, or 256 bit keys. These sessions are conducted using TLSv1. NSM hosts user console sessions using an Apache web server and cryptographic support is provided through an OpenSSL module interacting with an RSA BSafe cryptographic library.

NSP Sensor to NSM Sessions- FCS_COP.1c

All TSF data passed between NSP sensors and the NSM platform are secured using TLSv1 sessions or SNMPv3 with AES-128 bit symmetric keys and a SHA-1 hash for message integrity. A shared secret is configured between the NSP Sensor and NSM components during initial configuration to establish a trust relationship.

NSM to McAfee Update Server Sessions– FCS_COP.1b

The McAfee Update Server provides threat signature updates to the NSM platform for the purpose of providing the most up to date threat knowledge for use in detection processes. These sessions are secured using TLSv1 with AES-128 bit keys. The Update Server authenticates to the NSM Server using a certificate prior to establishing the session.

Hashing – FCS_COP.1d

The TOE performs hashing for integrity checking of TLSv1 session data between TOE components and the McAfee Update server using the SHA-1 hashing algorithm. The TOE hashes user traffic files smaller than 1MB using the MD5 algorithm. That hash is queried against the Artemis and/or user defined internal database[4].

RSA Key Wrap/Unwrap – FCS_COP.1e

The sensor verifies the signature updates (with the McAfee update server in the environment) by checking the digital signature using RSA.

RSA key wrap is used during the RSA key exchange that takes place during the TLSv1 session negotiation process for Console sessions with NSM and for NSM to NSP Sensor communications.

SSL Decryption – FCS_COP.1f

Sensors (other than M-series and I-1200 and 1400) are capable of intercepting SSL-encrypted traffic and (assuming the key pair has been loaded onto the TOE) decrypt, analyze, block traffic as configured.

7.7 System Data Collection

IDS_SDC.1 System Data Collection

The collection subsystem is used to detect events while monitoring the target network. Upon detection of such events, the collection subsystem generates data which is sent to the NSM for storage in the system database. For each event detected, the collection subsystem records and the NSM stores the date and time of the event, type of event, subject identity and the outcome (possible success, success, or failure) of the event with additional details for each event.

The NSM allows Security Administrators to establish new rules to detect new vulnerabilities, allowing complete control over the types of traffic that will be monitored and to set rules to govern the collection of data regarding potential intrusions.

For Network Traffic Events, the Protocol, Source Address and Destination Addressed are collected in audit records. For Vulnerability Detection Events, the identifier of the known vulnerability is listed in the audit records.

[4] Artemis functionality (including user defined signature verification) is only available using M-Series sensors.

7.8 System Data Analysis

IDS_ANL.1 Analyzer Analysis

To analyze the data collected by the Sensor, the NSM management platform uses defined signatures, protocol standards criteria and configured rules to identify potential malicious activity. A signature is the protection profile term for a rule. They are patterns of traffic corresponding to known attacks or misuses of a System.

The TOE is provided with default signatures for known exploits and the Security Administrator can add new signatures or detection rules at any time. New signatures are obtained from the Update Server as they are created and made available or imported from a SNORT signature. New signatures can be manually created by an administrator authenticated in the Security Administrator role.

Exploit detection may include “protocol violations” where packets do not conform to network protocol standards. (For example, they are incorrectly structured, have an invalid combination of flags set, or contain incorrect values.) This determination is done through parameter checking techniques such as parameter length checks.

Specific files are also blocked from passing through the sensor subsystem based on the signature set deployed within the TOE. The sensor subsystem creates an MD5 hash of suspect files and queries these “fingerprints” against the Artemis database. If this results in a match, the traffic is acted upon as configured. Security Administrators can also import custom MD5 signatures to be used in addition to the Artemis database.[5]

The TOE supports all analytical activities on SSL encrypted traffic, if the correct encrypting certificate is imported.[6]

When a pattern of traffic has been matched to a signature, protocol anomaly or detection rule, the specific event is recorded in the traffic log where it can be viewed and analyzed by users authenticated in the Security Expert role. The events are logged with the following information: the category of event and signature match, the time of the event, the data source and a copy of the packets used to identify the pattern.

A pattern of traffic that meets a signature is called an “alert.” The Threat Analyzer interface is used for the analysis of the alerts detected by NSP Sensors. Alert details include transmission information such as source and destination IP addresses in the packet and security analysis information (performed by the sensor) such as attack severity and type. Alerts are backed up to the NSM database and archived in order of occurrence.

For detailed analysis of alert information, the Threat Analyzer provides a “Drill Down” graphical administrative interface. Drill Down provides the Security Administrator with the capability to review statistical, signature, threshold, and anomaly-based functions by port scan. Alert information is organized by category of alert as follows:

- Severity: by severity,

[5] Artemis functionality is only available using M-Series sensors.

[6] This does not apply to I-1200, I-1400, or any M-series sensor models as these sensors do not support SSL decryption.

- Attack: by attack name,
- Source IP: by source IP addresses,
- Destination IP: by destination (target) IP addresses,
- Interface: by the sensor interface where alerts were captured,
- Domain: by admin domain where alerts were captured,
- Type: by attack type,
- Sensor: by the sensors where alerts were captured, and
- Application Protocol: by the application protocol of the detected attack

The "Time View" provides a view of the alert count during a specific time period. Time periods are expressed in date and time range. The Threat Analyzer provides an interface to view alerts in real time as they occur and a historical view. The historical view sets the filter to retrieve information for both acknowledged and unacknowledged alerts archived in the database during a specified time. The historical view does not refresh with new alerts as they occur.

The Threat Analyzer provides a view to analyze an individual alert called the "Alert Details." The Alert Details interface lists all of the alerts for the selected time span in order of occurrence, with most recent being listed first. Alert details are presented in multiple named columns, known as *attributes*. The attributes represent packet fields such as source and destination IP and sensor analysis fields such as attack severity and type.

The attributes in the Alert Details are as follows:

- Acknowledged: for Historical View, indicates state of recognition. If unchecked by an administrator, then the alert has not been manually acknowledged,
- Deleted: for Historical View, indicates if the alert has been selected for deletion during current analysis session,
- Time: time when the alert occurred. Alerts are listed from most (top of the list) to least (bottom) recent,
- Severity: system impact severity posed by the attack,
- Attack: specific name of the attack that triggered the alert,
- Source IP: IP address where the attack originated,
- Source IP Port: port on source machine where attack originated,
- Destination IP: IP address the attack was targeting,
- Destination IP Port: port on target machine where attack was destined,
- Domain: admin domain in which the attack was detected,
- Sensor: ID (*name*) of the sensor from where the alert was generated,
- Interface: sensor interface where the attack was detected, and
- Type: the type of attack. The choices are:

  - Exploit: an attack matching a known exploit attack signature.
  - Host Sweep: a reconnaissance attack attempting to see which IP addresses have live systems attached to them.
  - Port Scan: a reconnaissance attack attempting to see what services a particular system is offering.
  - Simple Threshold: denial of service attack against a set threshold limits.
  - Statistical: denial of service attack based on a learning statistical traffic profile.
- Throttle: a number of the same Signature attack occurring that exceeded an established limit suppression threshold in a designated period.

Report Generator Application

The Report Generator is a component of the NSM that is used to view and organize alerts.

IPS Reports

The Report Generator's IPS reports detail the network alerts generated by NSP Sensors. Alert reports are summaries based on specific types of information such as the source/destination IP of an attack, attack name, or time of alert. The TOE includes several pre-formatted reports for simple information gathering including an Executive Summary report which provides a high-level view of alert activity.

These IPS reports provide information on the alerts generated from the installed NSP Sensors. The generated alert information can include source and destination IP of the attack, time when attack occurred and the Sensor that detected the attack. Each report lists alerts from most to least common detected.

All IPS reports can be viewed in either HTML or PDF format. Specific reports can also be viewed in bar graph or pie chart format.

Configuration Reports

Configuration reports provide information on the settings configured using the Configuration page. The Security Administrator role user can generate reports to view the current software and signature versions, the status of a Sensor, policy and rule set configurations or proxy server settings. These reports provide a snapshot of the system's current configuration.

Scheduled Reports

Scheduled reports automate IPS report generation for convenient forensic analysis of the alerts generated by Sensors. The tool allows custom template generation. Reports can be scheduled to be generated and emailed on a daily or weekly basis.

IDS_RCT.1 Analyzer React

When signature matches are found, they can either be logged for later use or set to trigger an alarm. Current log entries can be viewed in real time by setting the "Real-time Log Viewer" values at the NSM console. Real-time viewing displays a limited number of entries as logged to the database. The number of entries to view can be selected and the refresh rate to refresh the console screen.

The NSM provides an interface to establish IDS security policies. A *security policy,* or IDS policy, is a set of rules that governs what traffic is permitted across your network, and how to respond to misuse of the network. An NSM *policy* is a set of rules/instructions defining the malicious activity that can be detected and the response. Creating a policy enables a Security Administrator to define an environment to protect by the different operating systems (OSs), applications and protocols in the network. These environment parameters or rules relate to all of the well-known attacks defended against by NSM.

All activities for which the underlying traffic content can violate an NSM policy may not be malicious, but may be explicitly forbidden by the usage policies of the network as defined by a security policy. A protocol violation can be an indication of a possible attack, but can also be triggered by malfunctioning software or hardware. Policy violations trigger alerts that are displayed on the NSM console.

The TOE uses Smart Blocking, which calculates the Benign Trigger Potential (BTP) of a particular signature and applies it to the overall attack. If an attack is sensed with a high BTP (high likelihood of false positive) the Security Administrator has the ability to specify the action to be taken by the sensor.

Alerts are asynchronous notifications sent when a system event or attack triggers the IDS. When a transmission violating a security policy is detected by a sensor, the sensor compiles information about the offending transmission and sends the information to the NSM in the form of an alert. An alert contains a variety of information on the incident that triggered it—such as the type of attack, its source and destination IP addresses, its source and destination ports, as well as security analysis information (performed by the sensor) such as attack severity and type. In addition to the alert that is generated, the IDS policy may be configured to ensure that the sensor responds by doing one or more of the following:

- Drop further packets (In-line mode only) — Dropping the specific attack packets is a key advantage of in-line mode. When detecting in-line (real time), the packets that trigger signatures and (optionally) all subsequent packets related to that connection are dropped before they reach the intended target system.
- Send an alert (default) — When traffic violates a Sensor policy, an alert is generated and sent to the NSM to be viewed using the Threat Analyzer. Alerts can be examined for content and sorted by key fields such as severity level, source and destination IP addresses etc.
- Host Quarantine action — Sensor performs the quarantine of infected host, by isolating the host for a specified period of time. Received packets from this host are dropped.
- Packet log — Sends a log, or copy, of the packet information to the NSM. This information acts as a record of the actual flow of traffic that triggered the attack and can be used for detailed packet analysis using Threat Analyzer.
- TCP reset — For TCP connections only. TCP uses the RST (Reset) bit in the TCP header to reset a TCP connection. Resets are sent in response to a connection that carries traffic which violates the security policy of the domain. The user can configure reset packets to be sent to the source and/or destination IP address.

- Alert filters — Alert filtering enables you to filter out alerts based on the source or the destination of the security event.
- ICMP host unreachable — ICMP Host Unreachable packets can be sent in response to the source of UDP or ICMP attacks.

7.9 System Data Review, Availability and Loss

IDS_RDR.1 Restricted Data Review

The NSM provides an interface where authenticated and authorized users can access the Threat Analyzer from the console workstation to view the traffic log data collected and analyzed by sensor.

IDS_STG.1 Guarantee of System Data Availability

IDS system data collected and analyzed by the NSP system is stored in a data store within the MySQL database and is protected from unauthorized deletion. TSF mechanisms prohibit any unauthorized user from modifying IDS data stored with the NSM.

IDS_STG.2 Prevention of System Data Loss

The NSM records the system data into a data store. The data store is running on the same dedicated platform as the NSM. The MySQL Database provides storage and retrieval for the system data.

All MySQL Database tables used for IDS data are dynamically allocated so that the limit on the recording capacity of the information is the limit of the physical disk partition on the platform dedicated to the MySQL Database data store.

When the storage capacity reaches 50%, 70%, and 90% of the configured IDS data monitoring limit (default 30M lines), an alarm is presented at the NSM console. The authorized administrator may then take action by using a graphical interface to copy the IDS data to another storage media. Read/Write access to IDS system data is limited to the Security Administrator role. This monitor registers the percentage of the configured “allocation” and not the actual drive space available which may be dynamically adjusted to make more storage available to the database.

If the MySQL Database tables that store the system data are exhausted, new system data will be ignored and an alert is generated to the Console.